Exhibit M

JUL 3 1 2017

Privileged & Confidential
Attorney-Client Communication

Hi Attorney Peachy, Tuesday, July 25th, 2017

I hope you are well and had a wonderful vacation. As per usual, please send me a copy of this letter through legal mail channels.

I've been pondering the upcoming motion and the larger strategy for the case. I have serious concerns about the zealousness of the defense and effectiveness of the assistance being provided to me by the Federal Defender's Office (FDO). I often feel the answers I'm told by the FDO are not in the pursuit of my best interests, but rather are geared towards avoiding making trouble for the U.S. Attorney's Office and/or the judiciary. For example, the FDO refused to make a filing and the stated reason was that my FDO attorney feared political ramifications. Shortly thereafter, that attorney accepted a more lucrative position in Washington D.C. on the Federal Sentencing Commission.

On various other occasions, the FDO has refused to take actions my previous attorneys routinely performed without hesitation. On nearly all of those occasions the stated reasons for such refusals had to do with supposed consequences, usually of a political nature, for FDO personnel. I feel that my requests spawn a process at FDO of searching for a reason why FDO can't fulfil my requests. Hmm.

I imagine that my current feelings regarding the FDO resemble those a calf who is aware of its surroundings

Privileged & Confidential
Attorney Client Communication

Tuesday, July 25th, 2017

and impending doom would have towered the slaughter-house workers attempting to coax it onto the conveyor belt. I feel the FDO is actually assisting the U.S. Attorney's Office and acting as a rubber stamp in my case.

I do not think the faith and trust I've lost in FDO are retrievable at this point. However, I do know if the government's acquiescence to the torture — as defined by Article 1 § 1 of the U.S.-ratified United Nations' Convention Against Torture — of Justin Pelletier is to be consigned to a mere footnote in our upcoming post-Swartz selective and vindictive prosecution motion, then I can no longer have even the smallest semblance of faith & trust in the FDO to represent me nor to engage in a fearless search for the truth.

Torture should never be relegated to a footnote and if our domestic case law leaves it no other place in this motion then that domestic case law is wrong and immoral and we should seek redress, if necessary by going inter alia to the 1st Circuit Court of Appeals. Indeed, the teeth of the upcoming motion should be government-sanctioned torture going unpunished in violation of the Convention Against Torture, while the person who acted morally in opposing that torture gets selectively and vindictively prosecuted by that same government. Against that backdrop, this prosecution cannot stand scrutiny and I feel the public has a right to know the above at this stage of the proceedings. I insist we take every opportunity

Privileged & Confidential,
Attorney-Client Communication

Tuesday, July 25th, 2017

to inform the public of such.

In any case, I ~~Further~~ insist on reading all motions with sufficient time before they are to be filed for me to have a say in revising them. Further, to go forward, I suggest the FDO confers with experts on the relevant Human Rights treaties. As a Senate-ratified binding treaty, the U.N. Convention Against Torture, commonly written as "CAT" in domestic case law, is the law of the land in the United States.

I refer the FDO to A/HRC/22/53 ¶ 24 regarding the U.S. Attorney's obligation under the CAT to "exercise due diligence" to prevent, investigate, prosecute, and punish" all CAT violations, even "those carried out" by non-State officials or private actors."

I refer the FDO to A/HRC/13/39/Add.5 ¶ 47 regarding the holding "that ~~the~~ concealment, such as hiding or destructing evidence of torture, has to be made an offence under criminal law."

Respectfully,

Martin Gottesfeld

Exhibit N

outlined below demonstrates that the explicit or implicit aim of inflicting punishment, or the objective of intimidation, often exist alongside ostensibly therapeutic aims.

2. The scope of State core obligations under the prohibition of torture and ill-treatment

23. The Committee against Torture interprets State obligations to prevent torture as indivisible, interrelated, and interdependent with the obligation to prevent cruel, inhuman, or degrading treatment or punishment (ill-treatment) because "conditions that give rise to ill-treatment frequently facilitate torture".[6] It has established that "each State party should prohibit, prevent and redress torture and ill-treatment in all contexts of custody or control, for example, in prisons, hospitals, schools, institutions that engage in the care of children, the aged, the mentally ill or disabled, in military service, and other institutions as well as contexts where the failure of the State to intervene encourages and enhances the danger of privately inflicted harm".[7]

24. Indeed, the State's obligation to prevent torture applies not only to public officials, such as law enforcement agents, but also to doctors, health-care professionals and social workers, including those working in private hospitals, other institutions and detention centres (A/63/175, para. 51). As underlined by the Committee against Torture, the prohibition of torture must be enforced in all types of institutions and States must exercise due diligence to prevent, investigate, prosecute and punish violations by non-State officials or private actors.[8]

25. In *da Silva Pimentel* v. *Brazil*, the Committee on the Elimination of Discrimination against Women observed that "the State is directly responsible for the action of private institutions when it outsources its medical services" and "always maintains the duty to regulate and monitor private health-care institutions".[9] The Inter-American Court of Human Rights addressed State responsibility for actions of private actors in the context of health-care delivery in *Ximenes Lopes* v. *Brazil*.[10]

26. Ensuring special protection of minority and marginalized groups and individuals is a critical component of the obligation to prevent torture and ill-treatment. Both the Committee against Torture and the Inter-American Court of Human Rights have confirmed that States have a heightened obligation to protect vulnerable and/or marginalized individuals from torture, as such individuals are generally more at risk of experiencing torture and ill-treatment.[11]

C. Interpretative and guiding principles

1. Legal capacity and informed consent

27. In all legal systems, capacity is a condition assigned to agents that exercise free will and choice and whose actions are attributed legal effects. Capacity is a rebuttable

---

[6] General comment No. 2 (2007), para. 3.

[7] Ibid., para. 15.

[8] General comment No. 2, paras. 15, 17 and 18. See also Committee against Torture, communication No. 161/2000, *Dzemajl et al.* v. *Serbia and Montenegro*, para. 9.2; Human Rights Committee, general comment No. 20 (1992), para. 2.

[9] Communication No. 17/2008, para. 7.5.

[10] Inter-American Court of Human Rights. (Series C) No. 149 (2006), paras. 103, 150; see also Committee on the Elimination of Discrimination against Women, general recommendation No. 19 (1992), para. 9.

[11] Committee against Torture, general comment No. 2, para. 21; *Ximenes Lopes* v. *Brazil*, para. 103.

44. While I fully respect and understand the fundamental security challenges with which many States are confronted, and express my full support for their legitimate and lawful endeavours to protect their citizens, it is somewhat astounding and instructive to see how many alleged "exceptional circumstances", "unique situations" etc. were presented to me in the course of the last five years. In many of my fact-finding missions, Government officials indicated that their country was currently confronted with an unrivalled and critical security challenge ranging from "global war on terror", internal armed conflict and secessionist movements to high rates of violent crime and drug offences. Against this background, officials of all ranks at least implicitly put the absoluteness and non-derogability of the torture prohibition into question and on some occasions portrayed it as an academic or theoretical, if not naïve ideal which lacks applicability and a sense of realism.

45. I have the honour to be entrusted with the mandate of the UN Special Rapporteur on torture during a period of time in which the absolute and non-derogable nature of the prohibition of torture was put into question for the first time since the existence of the United Nations, even in democratic States. It is and remains my firm belief that it was for good philosophical and historical reasons that States agreed in the aftermath of the Nazi Holocaust that the prohibition of torture should be guaranteed under international human rights law as one of the few absolute and non-derogable rights. History, including the recent context of the global "war on terror" shows that putting the absolute prohibition of torture in question means opening Pandora's Box. The present Administration of the United States of America has taken decisive steps to reverse this policy, but it will take many years until the global damage that was inflicted on the prohibition of torture as a rule of *jus cogens* is repaired.

(d) Torture as a crime

46. The gravity of torture finds a further consideration in the obligation, rare for a human rights treaty, to "ensure that all acts of torture are offences under its criminal law". This provision in article 4 CAT requires the criminal responsibility of any person who directly or through "complicity or participation" inflicted or only attempted to inflict torture. States have to make these offences punishable by appropriate penalties which take into account their grave nature.

47. The formulation "complicity or participation" also includes the incitement, instigation, superior orders or instructions, consent, and acquiescence, in line with the definition of torture in article 1(1). A study of the travaux préparatoires of the Convention also makes it clear that concealment, such as hiding or destructing evidence of torture, has to be made an offence under criminal law. Superior officials shall be held accountable under criminal law for their complicity or acquiescence if they knew or should have known that torture was inflicted by personnel under their command.[18]

48. Domestic criminal law has to cover all possible cases falling under the definition of torture as stipulated in the Convention. While it remains at the discretion of each Government how it wishes to live up to this requirement, my experience during the last five years leads me to the conclusion that it is difficult, if not impossible, to cover all the different aspects included in article 1 without explicitly incorporating this definition into the domestic criminal code.[19]

49. Hand in hand with the obligation to criminalize torture goes the obligation to punish perpetrators with *sentences commensurate to the gravity of the crime*. Torture is not a

[18] On the concept of acquiescence see also the case of *Hajrizi Dzemajl et al. v. Yugoslavia*, No. 161/2000, para. 9.2 and 10. See below, article 16, 2.2.

[19] CAT/C/SR.268, para. 2.

 Exhibit P

FEDERAL DEFENDER OFFICE
DISTRICT OF MASSACHUSETTS
51 SLEEPER STREET, FIFTH FLOOR
BOSTON, MASSACHUSETTS 02210

TELEPHONE: 617-223-8061
FAX: 617-223-8080

August 2, 2017

Martin Gottesfeld
Reg. #12982-104
Plymouth County Correctional Facility
26 Long Pond Road
Plymouth, MA 02360

RE: United States v. Martin Gottesfeld
Criminal No. 16-10305-NMG

Dear Marty:

I am writing in response to your most recent letter. I am sorry that you feel that my office is not doing everything we can to defend you. We are. You may not like what we tell you, but it is our obligation to be honest with you and not to just tell you what you want to hear. I will say just two more things at this time. One, you are free to file a motion with the court to have me, and my office, withdraw from our representation of you and to request another attorney. Two, while I will do my best to accommodate your various requests, it is ultimately up to me, the lawyer, to decide what motions and arguments have merit and what to file with the Court. I am working diligently to find arguments that have merit and support in the law to include in your motions. Ultimately, the decision what motions to file, and what to include in those motions, is mine, not yours. The decisions in the case that are yours are as follows:

(i) whether to proceed without counsel;
(ii) what pleas to enter;
(iii) whether to accept a plea offer;
(iv) whether to cooperate with or provide substantial assistance to the government;
(v) whether to waive jury trial;
(vi) whether to testify in his or her own behalf;
(vii) whether to speak at sentencing;
(viii) whether to appeal; and
(ix) any other decision that has been determined in the jurisdiction to belong to the client.

I will come meet with you soon to discuss what motions we will be filing, but I wanted to clarify our roles in this case first.

Sincerely,

/s/ Jane F. Peachy
Jane F. Peachy
Assistant Federal Defender

JFP/rk

Exhibit Q

Is The FBI Using Intimidation Tactics Against Wife Of Justina Pelletier's Guardian Hacktivist?

Posted at 11:30 am on August 4, 2017 by Jim Jamitis

Dana Gottesfeld, the wife of imprisoned hacktivist Marty Gottesfeld claims that the FBI is using intimidation tactics against her. She says they are threatening to investigate her unless she takes down YouTube audio of testimony given by an FBI special agent at a detention hearing for her husband.

Dana says the FBI has ominously warned her that recording court proceedings is illegal and they will have to investigate her if it is not removed from YouTube, but the recording she posted was obtained legally through the court.

The testimony is embarrassing to the FBI because it shows that they have done nothing to investigate the "medical kidnapping" of Justina Pelletier, which Michelle Malkin recently investigated.

> Dana's husband, Marty, faces felony charges of computer hacking and conspiracy related to distributed denial-of-service (DDoS) attacks in April 2014 against Boston Children's and the nearby Wayside Youth and Family Support Network residential treatment. Marty had organized a social-media army to knock the computer networks of both institutions offline to protest the medical kidnapping of then-15-year-old Justina Pelletier. Hackers from the loose-knit collective, Anonymous, allegedly participated in the campaign.
>
> Justina's plight had become international news in Marty's backyard. One fateful winter day in February 2013, Justina traveled with her mom to BCH from her West Hartford, Conn., home, seeking relief from a severe case of the flu. Ordinary sickness compounded Justina's rare medical conditions, including mitochondrial disease and postural orthostatic tachycardia syndrome. But those illnesses hadn't stopped her from participating in school, competitive ice skating, and an active family life.
>
> Instead of receiving top-notch care and attention at BCH, however, Justina was snatched from her parents and recklessly rediagnosed with a psychological condition, "somatoform disorder." She was dragged from BCH's neurology department to its infamous psych ward, where she was reprimanded for being unable to move her bowels or walk unassisted in her weakened state. At Wayside, she was harassed by a staffer while taking a shower. The physical and mental torture lasted 16 months.

TRENDING

1 *SCANDAL. Donald Trump Is Handicapping Supreme Court Vacancies*

2 *Hillary Clinton Is Nearly Right About This One Thing*

3 *Trump's Cheap "Merry Christmas" Christianity Continues to Sway Evangelicals*

4 *Paul Ryan Blows Off Bannon's Declaration of "War"*

5 *Is a War Brewing Between Iraqi Kurdistan and Iran?*

SCANDAL. Donald Trump Is Handicapping Supreme Court Vacancies

streiff

Kaepernick to NFL Owners: You've Colluded Against Me!

Susan Wright

Jimmy Kimmel Does Not Want to Talk to You

Patterico

Exhibit R

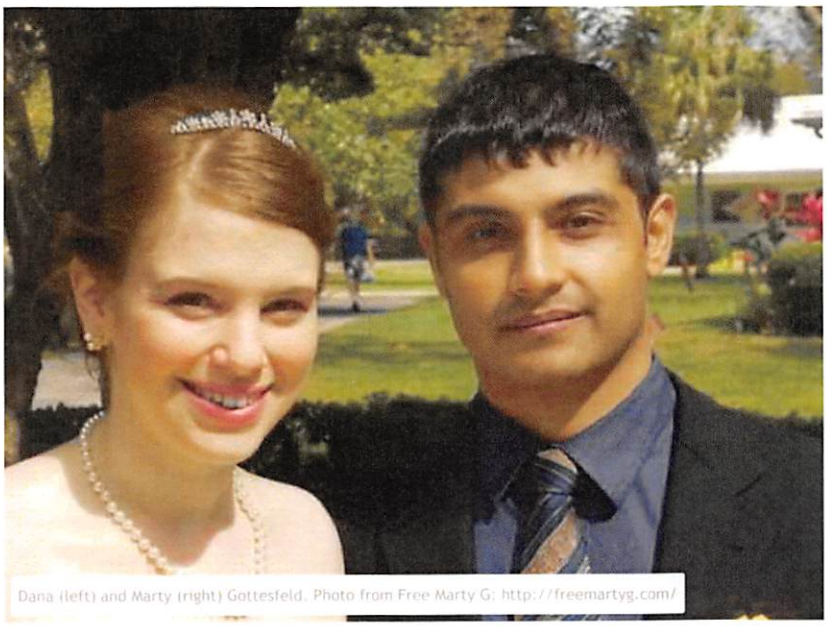
SHADOWPROOF

DISSENTER FEATURED / LATEST NEWS / THE DISSENTER

PROSECUTOR DEMANDED TAKEDOWN AFTER WIFE OF INCARCERATED ACTIVIST PUBLISHED LEGALLY OBTAINED COURT RECORDING

07 AUG 2017 |  KEVIN GOSZTOLA

♡ 5 4



Dana (left) and Marty (right) Gottesfeld. Photo from Free Marty G: http://freemartyg.com/

23

The wife of an activist, jailed for engaging in a digital sit-in against the Boston Children's Hospital website, says she was threatened by the FBI for posting a clip of sworn testimony from the case to YouTube.

Marty Gottesfeld learned about the case of Justina Pelletier, who was institutionalized in a psychiatric ward in 2013 against her parents' wishes. Gottesfeld allegedly organized with members of Anonymous and participated in a distributed denial of service (DDOS) operation that disrupted the donation portal for the hospital website.

He was arrested in Miami in February last year and faces a conspiracy charge and charges of "intent to damage a protected computer," which are offenses under the Computer Fraud and Abuse Act. If convicted, he faces up to 25 years in prison and could pay hundreds of thousands of dollars in restitution.

Dana Gottesfeld purchased a copy of a court recording of his detention hearing. She published a snippet of audio to YouTube—a statement from the hearing in which FBI Special Agent Jeffrey Williams states the FBI was not investigating abuse of Pelletier.

A prosecutor from the U.S. Attorney's Office in the District of Massachusetts suspected it was an unauthorized recording and requested Dana Gottesfeld take the clip down. If she did that, the prosecutor would promise not to investigate the matter or raise the issue with the federal judge in the case.

She thinks it is highly likely the FBI is closely monitoring postings from the "Free Marty G" campaign and anything that appears on the internet about him.

"What the FBI is threatening to do to me is a microcosm of what they are doing to Marty, another instance of selective exercise of their powers," Dana Gottesfeld told Shadowproof. "I would sincerely hope that instead of coming after me for a recording that I legally bought from them that they investigate Boston Children's Hospital for allegations they admitted they are aware of against Justina Pelletier."

"What is their beef with squashing those who point out that Boston Children's Hospital is abusing children and instead using the almighty power of the United States Attorney's Office to protect their friends, the abusers?"

Marty Gottesfeld also issued a statement, "The Boston FBI and U.S. Attorney's office under President [Barack] Obama allowed Justina Pelletier to be tortured and maimed by their Harvard-affiliated political allies at Boston Children's Hospital. Then, they sought vengeance on behalf of those allies by bringing a case against me to a judge also closely aligned with the hospital."

"Now, with their corruption imploding around them, they have taken to threatening my wife in a vain attempt to suppress the truth. I implore the public not to let them succeed and ask the new administration to please end this travesty by instead investigating the torture of Justina," Marty Gottesfeld added.

The U.S. Attorney's Office is the same office that Carmen Ortiz once oversaw as a U.S. Attorney. Ortiz was responsible for the zealous prosecution of Aaron Swartz for alleged violations of the Computer Fraud and Abuse Act. The prosecution only came to an end when Swartz committed suicide.

Under Ortiz, the same office developed a reputation for overreach or abuse of power: indicting Tim Sullivan, an aide to Boston Mayor Marty Walsh, for refusing to grant permits for a music festival until union hands were hired; charging a U.S. Customs Service receptionist with "inducing" an undocumented immigrant—her housekeeper—to remain in the country; subpoenaing the Belfast Project, "a Boston College archive of oral histories from former fighters on both sides of the late 20th century civil war in Northern Ireland."

Marty Gottesfeld is in pretrial detention, and the trial is scheduled for January 2018.

23

TAGS: FBI JUSTICE DEPARTMENT MARTY GOTTESFELD

PREVIOUS POST
INTERVIEW WITH AMAL SAAD ON HEZBOLLAH AND LIBERATION OF LEBANON FROM AL QAIDA

NEXT POST
PROTEST SONG OF THE WEEK: 'BLOOD MONEY' BY PROTOJE

KEVIN GOSZTOLA

Kevin Gosztola is managing editor of Shadowproof Press. He also produces and co-hosts the weekly podcast, "Unauthorized Disclosure."

YOU MIGHT ALSO LIKE

Photo by Mike Kemp/In Pictures via Getty Images

Wife Of Jailed Hacktivist Claims FBI Is Threatening Her To Take Down YouTube Video

Exhibit S

"It's a thinly veiled threat, typical Obama-style weaponized DOJ intimidation."

By AARON BANDLER

August 9, 2017 34.4k views

The wife of jailed hacktivist **Martin Gottesfeld (http://www.dailywire.com/news/15158/exclusive-federal-government-wouldnt-let-aaron-bandler)**, Dana Gottesfeld, is claiming that the FBI is threatening to force her to take down an audio clip on YouTube.

Martin Gottesfeld is currently in jail for using hacking as a means to raise awareness to the plight of teenage girl Justina Pelletier, who was taken away from her parents by the Boston Children's Hospital because they claimed that she didn't have mitochondrial disease, insisting instead that she had mental health issues. She resided in the hospital and Wayside Youth and Family Support Network under horrific conditions, the family claims, so Gottesfeld hacked their websites in response to their actions to highlight what was going on.

The YouTube audio clip in question is of an FBI special agent admitting that they didn't investigate what was done to Justina:

Gottesfeld told *The Daily Wire* in an email that she was told by her husband's attorney that the prosecutors might be going after her for posting the clip because it's illegal for a private citizen to record in a federal courthouse. Christina Sterling, the spokesperson to the Boston U.S. Attorney's office, told *The Daily Wire* in an email that the prosecutors are indeed planning on bringing up the audio clip in court for violating those rules.

But Gottesfeld claims that she received the audio clip through the court reporter supervisor, a claim she substantiated by sending *The Daily Wire* an email exchange between her and the court reporter supervisor.

When pressed by *The Daily Wire* as to how Gottesfeld violated the rules by receiving the audio from the court reporter supervisor, Sterling simply responded: "The court will have to make that determination."

Gottesfeld claimed that the Boston FBI first raised the issue, and that "the Obama holdovers at the Boston U.S. Attorney's office are the mouth piece for his holdovers still at the Boston FBI."

"It's a thinly veiled threat, typical Obama-style weaponized DOJ intimidation," Gottesfeld wrote to *The Daily Wire*. "Back when they were initially investigating Marty, they also went out to my parent's home in Los Angeles to intimidate them, all typical J. Edgar Hoover-esque intimidation methods to control and silence."

Martin Gottesfeld sent the following statement, which was also shared with *The Daily Wire*:

> The Boston FBI and U.S. Attorney's office under President Obama allowed Justina Pelletier to be tortured and maimed by their Harvard affiliated political allies at Boston Children's Hospital. Then, they sought vengeance on behalf of those allies by bringing a case against me to a judge also closely aligned (http://www.dailywire.com/news/15158/exclusive-federal-government-wouldnt-let-aaron-bandler#exit-modal) with the hospital. Now, with their corruption imploding around them, they have taken to threatening my wife in a vain attempt to suppress the truth. I implore the public not to let them succeed and ask the new administration to please end this travesty by instead investigating the torture of Justina. Please go to FreeMartyG.com (https://freemartyg.com/) for more information.

H/T: (http://www.redstate.com/jimjamitis/2017/08/04/fbi-using-intimidation-tactics-wife-justina-peltiers-guardian-hacktivist/) *RedState*

Follow Aaron Bandler on Twitter. (https://twitter.com/bandlersbanter)

Exhibit T

More Judicial Conflicts Of Interest In The Case Of Justina Pelletier's Guardian Hacktivist

Posted at 4:24 pm on August 15, 2017 by Jim Jamitis

Earlier this year I wrote about hacker Marty Gottesfeld being denied bail by Magistrate Judge Marianne Bowler who has ties to Harvard Medical School who runs the hospital Marty is alleged to have hacked in response to the medical kidnapping of Justina Pelletier. She determined that Gottesfeld is a "flight risk."

(For perspective, note that Debbie Wasserman Schultz's IT contractor who was arrested for fraud *while literally attempting to flee the country* was released with a GPS monitor while Gottesfeld has been sitting in prison for years awaiting trial.)

Now it looks like Bowler has an even bigger conflict of interest in this case. Bowler is a an emeritus member of the board of directors for The Boston Foundation, a philanthropic foundation who gives money to the Wayside Youth and Family Support Network who along with Boston Children's Hospital is the target of the Pelletier family's lawsuit over the medical kidnapping of their daughter Justina.

BOARD OF DIRECTORS

Current Members	Emeritus Members
Michael Keating, *Chair*	Dwight L. Allison, Jr.
Paul A. La Camera, *Vice Chair*	Carol F. Anderson
Rosalin Acosta	Joan T. Bok
Zamawa Arenas	The Honorable Marianne B. Bowler
Sandra Edgerley	Richard M. Burnes, Jr.
Michael Eisenson	Louis Casagrande
Grace Fey	Gerald Chertavian
Paul C. Gannon	Catherine D'Amato
Rev. Gregory Groover	Richard DeWolfe
	The Honorable Barbara A. Dortch-Okara

Thankfully, the troublingly compromised Bowler is not the trial judge for Gottesfeld's case. That will be one of the more conservative federal judges in Massachusetts, Nathanial M. Gorton. Gorton was the Boston judge who ruled to discontinue the restraining order against President Trump's executive order that paused travel from seven predominantly Muslim countries until vetting procedures could be reviewed.

TRENDING

1 *SCANDAL. Donald Trump Is Handicapping Supreme Court Vacancies*

2 *Trump's Cheap "Merry Christmas" Christianity Continues to Sway Evangelicals*

3 *Hillary Clinton Is Nearly Right About This One Thing*

4 *The RedState Box Office Report*

5 *Paul Ryan Blows Off Bannon's Declaration of "War"*

SCANDAL. Donald Trump Is Handicapping Supreme Court Vacancies

streiff

Kaepernick to NFL Owners: You've Colluded Against Me!

Susan Wright

Jimmy Kimmel Does Not Want to Talk to You

Patterico

Exhibit U

JUSTICE FOR JUSTINA

WHY THE FBI THREATENED MY WIFE OVER A YOUTUBE CLIP

Exclusive: Martin Gottesfeld shares latest development in girl's 'medical horror story'

Published: 08/18/2017 at 7:24 PM

image: http://www.wnd.com/wp-content/plugins/wp-print/images/printer_famfamfam.gif

Print

By Martin Gottesfeld

Note: Martin Gottesfeld was featured by columnist Michelle Malkin for defending Justina Pelletier when she was maimed at Harvard-affiliated Boston Children's Hospital (BCH), leading to his imprisonment without bail by a Harvard-affiliated judge and Obama-appointed prosecutors. See FreeMartyG.com, the FreeMartyG Facebook page and the @FreeMartyG Twitter account for more info.

image: http://www.wnd.com/files/2017/08/justina44.jpg

Pelletier family photos

A picture is worth a thousand words. Both photos above are of a girl named Justina Pelletier. On the left, she's ice skating while under her parents' custody. On the right, a short time later, she's confined to a wheelchair thanks to Boston Children's Hospital (BCH) and social services in the Commonwealth of Massachusetts.

On the left, Justina's parents were getting her care from some of the best experts in the world for her potentially crippling and deadly case of mitochondrial disease, the same condition that was at issue recently with baby Charlie Gard in the U.K. When that photo was taken Justina was a competitive figure skater coached by her older sisters and her mother, who was a champion skater herself. The sport is in Justina's blood, and she loves it.

On the right, we see Justina after she was medically kidnapped from her parents by Boston Children's Hospital. You see, a group of so-called "experts" there, starting with a young neurologist seven months out of medical training named Jurriaan Peters, took exception to her mitochondrial disease, or "mito" diagnosis. So, they asked her parents to agree to stop her mito therapies, including her badly needed pain killers, and when they refused, the hospital called child protective services. BCH told them the Pelletiers were "medically abusing" Justina by treating her for mito instead of a psychological condition its staff wrongly thought she had.

Eleven months later Justina was moved to a nearby facility for mentally troubled youth called Wayside, where she continued to be treated by the BCH plan – and not for mito. As Michelle Malkin found in her recent investigation:

> Instead of receiving top-notch care and attention at BCH, however, Justina was snatched from her parents and recklessly rediagnosed with a psychological condition, "somatoform disorder." She was dragged from BCH's neurology department to its infamous psych ward, where she was reprimanded for being unable to move her bowels or walk unassisted in her weakened state. At Wayside, she was harassed by a staffer while taking a shower. The physical and mental torture lasted 16 months.

When the Pelletiers tried to have Justina's original doctors see her at BCH, the hospital refused to let them or other independent specialists examine her.

When a local Fox TV crew set up outside the juvenile court where Justina's fate was being decided behind closed doors, her father reported BCH was "up in arms," and an unconstitutional gag order was quickly issued, violating the Pelletiers' First Amendment rights (as well as the rights of a free press) by barring them from speaking to the media. They were also forbidden from photographing Justina and thereby visually documenting her horrifying and painful deterioration without her mito treatments.

At BCH's insistence, Justina and her family were even ordered not to discuss her condition nor care during their once per week hour-long visits (supervised by armed guards) and 20-minute monitored weekly phone calls.

Justina, a Catholic, wasn't allowed to attend Mass, take Communion, nor go to Confession.

In addition to all these First Amendment violations, Justina's federal right to an education in the least restrictive setting possible was also violated and she fell years behind her classmates. More than 14 months into this travesty, many people, including Justina herself, were terrified she was going to die before the

reputation-obsessed, $2 billion, Harvard-affiliated BCH admitted it was wrong and let her go or found a way to end this situation while saving face.

By the end, nearly everyone, including BCH, seemed to understand the psychological diagnosis was wrong, but that didn't stop the hospital from continuing to accept tens, if not hundreds of thousands of federal Medicaid dollars to "treat" Justina for it. While elsewhere in the country doctors taking government money to treat a patient for a condition they know she doesn't have would worry about being arrested for federal health-care fraud, as demonstrated by the $225 million in annual federal funding BCH receives (the most of any pediatric research facility in the nation), BCH is one of the best-connected political entities in Massachusetts. Further protecting it, BCH then shared its Harvard affiliation with the governor of Massachusetts, the top federal prosecutor in Boston and even former President Barack Obama. Indeed, the Pelletiers were dismayed when even the "independent" adviser their juvenile court judge appointed to guide him through the medical details in the case listed an affiliation with BCH in her email signature.

image: http://www.wnd.com/files/2017/08/gottsefeld170819.jpg

WELL-CONNECTED: Boston Children's Hospital (BCH) shares a close connection to Harvard University with former Massachusetts Gov. Deval Patrick (top-left), former U.S. President Barack Obama (middle), former Boston U.S. Attorney Carmen Ortiz (top-right), and current Acting Boston U.S. Attorney William Weinreb (bottom). Clockwise (from top-left): Scott LaPierre/ CC By 2.0, Public Domain, Public Domain, Pete Souza/Public Domain

Unsurprisingly, when the Pelletiers asked, no law enforcement agency nor other government body would help them, including the Boston FBI – which brings us to the YouTube clip below and the Bureau's threat to "investigate" my wife if she refused to take it down. The clip was legally recorded and obtained. It's from FBI Agent Jeffrey Williams' sworn court testimony and confirms that though the Boston feds know about the horrible things Justina and her parents report were done to them, they didn't investigate BCH nor Wayside.

When that testimony was first given in April 2016, the Boston FBI also proudly told a biased judge the feds had hand-selected that though they let Justina suffer for over a year without lifting a finger to protect her, they immediately began investigating my defense of her life. They were forced to admit that unlike what their allies had done to Justina, my actions in her defense didn't harm a soul.

In a further irony that seems totally lost on the feds, while they still refuse today to investigate the awful things their cronies did to Justina, they recently reacted to this clip by threatening to "investigate" my wife for posting it and refusing to take it down. That's the best demonstration yet of the DOJ's crookedness in this case and shows that even if public shame eventually forces them to "investigate" what put Justina in that wheelchair to this day, these holdovers, including Acting Boston U.S. Attorney William Weinreb, himself a Harvard grad, cannot be trusted to do so honestly.

So, in their own battle to get some small bit of justice, around the time of the FBI's admission above, Justina's family filed a lengthy lawsuit against BCH and the doctors who maimed her. It reads like a medical horror story.

When the Pelletiers announced they were suing, Justina, the one-time athlete told the world, "I really, really want to walk again and skate."

She also joined thousands of supporters by saying the following about her BCH doctors: "I just really, really want them to get what they deserve."

However, no lawsuit can see to that, and if the current folks at the Boston DOJ get their way, nothing else will either. But, when Agent Williams was on the stand in April 2016, he and his colleagues couldn't care less about their corruption being exposed – and now they are desperate to get that clip taken down. I wonder, what's changed between then and now? Any guesses?

image: http://www.wnd.com/files/2017/08/gottsefeld170819a.jpg

On Jan. 20, 2017, Donald J. Trump (left) was sworn in as the 45th president of the United States, and on Feb. 9, 2017, Jeff Sessions (right) was sworn in as his attorney general.

Read more at http://www.wnd.com/2017/08/why-the-fbi-threatened-my-wife-over-a-youtube-clip/#3U6EKwcmr25C8WZQ.99

Exhibit V

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**DOCKET NO. 16-CR-10305-NMG**
	)	
MARTIN GOTTESFELD	)	

MOTION TO SUPPRESS EVIDENCE

Martin Gottesfeld moves to suppress evidence obtained by the government as a result of their execution of a search warrant for his Somerville apartment on October 1, 2014.[1] The search warrant relied upon information derived from the government's warrantless, constant, real-time and long-term surveillance of Gottesfeld's internet activity. This information was obtained in violation of Gottesfeld's Fourth Amendment rights. Absent this illegally obtained information, the search warrant fails to establish probable cause to believe evidence of a crime would be found in Gottesfeld's apartment and that seizure of all computers and electronic devices in that home was necessary. For these reasons, Gottesfeld seeks to suppress from evidence at trial any items taken from his home during the execution of the search warrant, and any information obtained by the government as a result of the seizure of those items.

BACKGROUND

The government obtained the search warrant for Gottesfeld's apartment after investigating a Distributed Denial of Service ("DDOS") attack on Boston Children's Hospital fundraising webpage on April 20, 2014. In their application for this search warrant, the government sets forth their belief that the DDOS attack was part of an "activist effort concerning the custody battle over teenage

[1] A copy of the search warrant and its application are attached as Exhibit A. All exhibits are filed under seal in accordance with the Protective Order pertaining to discovery in this case. *See* D.E. 43 (Nov. 21, 2016).

medical patient Justina Pelletier." Ex. A. at ¶9. They cite a YouTube video titled "Anonymous #OpJustina Press Release Video" which was posted from a YouTube account belonging to Martin Gottesfeld on March 23, 2014. *Id.* at ¶¶10, 16. This video, which claimed to be from the group Anonymous, stated that Anonymous "will punish all those held accountable and will not relent until Justina is free," ordered Children's Hospital to terminate the employment of one of the doctors involved in Justina Pelletier's treatment, and warned "Test us and you shall fail." *Id.* at ¶¶11, 12. The video concludes with a link to a website that had the address, phone number, website address, and IP address for Boston Children's Hospital. *Id.* at ¶13. Agents learned that the YouTube video was posted using an IP address belonging to Martin Gottesfeld. *Id.* ¶17.

On July 17, 2014, three months after the DDOS attack on Children's Hospital, the government obtained a pen register/trap and trace order from the Court allowing them to collect, in real-time, the IP addresses sending communications to, and receiving communications from, Gottesfeld's IP address for 60 days.[2] The order also allowed the government to obtain the subscriber information associated with each IP address communicating with Gottesfeld's IP address.

From that the order, the government gathered information that showed that Gottesfeld was using a VPN service through the website www.riseup.net, and also that he was using the TOR network. Ex. A. at ¶¶22, 24. The government noted this information in their search warrant application and also noted that two Twitter accounts that had posted about the Children's Hospital DDOS attack used these same services. *Id.* at ¶25. The government also noted that criminals frequently use these types of anonymizing services to mask their criminal activities. *Id.* at ¶26.

The government also learned that Gottesfeld was an outspoken activist against the troubled teen industry and was critical of other institutions that abused and mistreated children residing at

[2] The application for the Pen Register/Trap and Trace Order is attached as Exhibit B. The order is attached as Exhibit C.

their facilities. Ex. A. at ¶¶28-31. Two of those institutions that Gottesfeld was critical of also experienced DDOS attacks. *Id.* at ¶¶39, 31.

On September 29, 2014, the government obtained a search warrant to search Gottesfeld's apartment in Somerville. The warrant authorized them to seize a long list of items, including all computer hardware (including tablets and smart phones), computer software, and storage media. When the police searched Gottesfeld's apartment on October 1, 2014, they took multiple computers, storage media, and Gottesfeld's smart phone. The police later examined those devices and discovered evidence implicating Gottesfeld in the DDOS attack against Children's Hospital.

I. THE WARRANTLESS SURVEILLANCE OF MR. GOTTESFELD'S INTERNET ACTIVITIES WAS UNLAWFUL AND MERITS SUPPRESSION

As part of its investigation, the government requested and obtained an *ex parte* order under the Pen Register/Trap and Trace Statute ("Trap/Trace"), 18 U.S.C. § 3121–27, and the Stored Communications Act ("SCA"), 18 U.S.C. § 2703. The former permitted it to have the Internet Service Provider ("ISP") install a Trap/Trace device that would trace the "source and destination of all electronic communications directed to or originating from" Gottesfeld's IP address and transmit that information to the government, "continuously," in real time, 24 hours a day for 60 days. *See* Ex. B at 1, 5. The latter enabled it to obtain the subscriber information for each IP address Gottesfeld communicated with. *See id.* § 2703(c)&(d). Below, Gottesfeld argues that the order exceeded statutory authority and that the surveillance constituted a search and seizure under the Fourth Amendment. He acknowledges authority to the contrary. Nevertheless, he maintains that the reality of modern technology consumption compels the conclusion that individuals have a reasonable expectation of privacy in their online activities. Furthermore, source and destination information, when aggregated over a long period of time, reveals constitutionally and statutorily protected "content" information. The Supreme Court is poised to revisit the third party doctrine, which has

heretofore insulated this information from Fourth Amendment protection, in *Carpenter v. United States*, S.Ct. No. 16-402 (cert. granted June 5, 2017).

A. THE FOURTH AMENDMENT PROHIBITS THE WARRANTLESS SURVEILLANCE OF AN INDIVIDUAL'S ONLINE ACTIVITY

1. Internet Information Is Protected by the Fourth Amendment Right to Privacy

Since at least 1967, the Supreme Court has recognized that the Fourth Amendment protects an individual's right to privacy, even in public places. *Katz v. United States*, 389 U.S. 347, 351 (1967). *Katz* held that when the government infringes upon a subjective expectation of privacy that society recognizes as reasonable, it effects a search and seizure within the meaning of the Fourth Amendment. *Id.* at 353. Thus, in *Katz*, the government was found to have violated the defendant's Fourth Amendment rights by eavesdropping on his private conversation in a public phone booth. *Id.*

In *United States v. Knotts*, the Court first applied the *Katz* test to electronic surveillance, holding that the Fourth Amendment was not violated when the government used a beeper to track a car. 460 U.S. 276, 277 (1983). The beeper tracking in *Knotts* did not implicate the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.... [By travelling on public streets] he voluntarily conveyed ...the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination...." *Id.* at 281. However, the Court left open the possibility that advances in surveillance technology would require it to reevaluate its decision. *Id.* at 283-84.

The following year, in *United States v. Karo*, the Court limited *Knotts* to electronic surveillance *in public places*. 468 U.S. 705, 714 (1984). In *Karo*, the police placed a beeper in a container belonging to the defendant and monitored its location electronically, including while it was inside a private residence. *Id.* at 708-10. The Court held that the monitoring of the beeper inside the home was an

unconstitutional trespass into the residence by electronic means. *Id.* at 715; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (Fourth Amendment violated by thermal imaging of a house).

In *United States v. Jones*, five Justices of the Court found that GPS monitoring of a car, in public places, for one month impinged on a legitimate expectation of privacy. 132 S. Ct. 945, 954 (2012); *id.* at 955 (Sotomayor, J., concurring); *id.* at 965 (Alito, J., concurring). In *Jones*, the government placed a GPS tracker on the defendant's car and used it to monitor the car's location – on public thoroughfares – for 28 days. *Id.* at 948. The majority opinion held that the government had violated the Fourth Amendment by the physical trespass of placing the tracker on the vehicle, and it therefore did not need to address whether the location tracking violated a reasonable expectation of privacy. *Id.* at 949. It explicitly noted, however, that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original).

The five Justices who did engage in a *Katz* analysis concluded that the government's actions in tracking the car's location violated the Fourth Amendment. *Id.* at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, Ginsburg, Breyer, & Kagan, JJ., concurring). Justice Sotomayor agreed that prolonged electronic surveillance violates the Fourth Amendment. *Id.* at 955. She added, however, that "even short-term monitoring" raises concerns under *Katz* because "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* She questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring). And Justice Alito wrote, for four justices, "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964.

Just as the government catalogued "every single movement" of Jones' car, as it travelled the physical world, the government here has surveilled "every single movement" of Gottesfeld's, as he travelled the internet. Both types of surveillance – GPS tracking of a car and internet tracking of destination IP addresses – reveal the destinations an individual visits, but not the activity s/he partakes in once s/he arrives at a given destination.[3] The surveillance simply sits dormant and waits until the individual leaves and goes to a different destination address. When grafted in small segments, the information revealed by such a search does not trigger the Fourth Amendment. *See Knotts*, 460 U.S. at 281 (no reasonable expectation of privacy in an individual's "movements from one place to another," "on public thoroughfares"). Yet we know from *Jones* that the same information, in the aggregate, becomes constitutionally cognizable. *See Jones*, 132 S. Ct at 956 (Sotomayor, J., concurring) (asking whether individuals have a reasonable expectation of privacy in the "sum of [their] public movements" or whether individuals reasonably expect that their public movements will be "recorded and aggregated in a manner that enables the Government to ascertain [a highly personal level of detail];" *id.* at 964 (Alito, J., concurring) (finding law enforcement's "catalogu[ing] every single movement of an individual's car for a very long period" constitutionally offensive). Here, the 24-hour, real-time surveillance of all of Gottesfeld's internet traffic, for 60 days, goes well beyond what ordinary people expect the government to be observing.

Alternatively, the surveillance in this case is constitutionally cognizable if viewed as the surveillance of *content* information. *See* § I.B below. The content of communications is protected

[3] Indeed, if the government is correct that its surveillance reveals that an individual visits Amazon.com, while not the particular book at Amazon.com, its surveillance reveals internet trips that are undeniably private. *Cf., e.g., People v. Weaver*, 12 N.Y.3d 433, 441–442 (2009) (noting, of GPS data, that it would disclose "trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on," *quoted in Jones*, 565 U.S. at 415 (Sotomayor, J.)). The same is disclosed by cyber visits to the internet analogue to those locations.

under *Katz*, 389 U.S. 347 (legitimate expectation of privacy exists in contents of phone conversation). *See Smith*, 442 U.S. at 741 (distinguishing between the "means of establishing communication," as revealed by the pen register's recording of the phone numbers dialed, and the "purport of a[] communication," as revealed by the recording of a conversation in *Katz*); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 135-36 (3d Cir. 2015) (discussing this distinction between "extrinsic information used to route a communication and the communicated content itself" as "loom[ing] large in federal surveillance law"). Gottesfeld contends that technology has rendered the seizure of internet "source and destination" information, Ex. B at 1, more comparable to content, under *Katz*, than to "means of establishing communication" under *Smith*. *But cf. United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that "e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers," while declining to "imply that more intrusive techniques or techniques that reveal more content information [would be] constitutionally identical to the use of a pen register"); *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017).

Further supporting the conclusion that Gottesfeld had a reasonable expectation of privacy in his online activities is the fact that he used encryption services – the only way an individual can attempt to hold on to his privacy while using the internet. *See* Ex. A at ¶¶ 22-24 (stating that Gottesfeld used riseup.net, a service that provides "location anonymization and traffic encryption," and The Onion Router (TOR), "another tool used to browse the internet anonymously"); *cf. Smith v. Maryland*, 442 U.S. 735, 743 (1979) (finding that a caller's decision to use the home phone, instead of a pay phone, "was not and could not have been calculated to preserve the privacy of the number he dialed"). Where Gottesfeld was using the internet inside his own home, on his own computer, and

further encrypting his activities, he expected that his online activities were private. Society recognizes that expectation as reasonable.

2. That expectation is not forfeited simply because internet usage occurs through the service of a third party

It would be incorrect to analogize the internet information at issue here to the bank records and pen registers held not subject to Fourth Amendment protections in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). *Smith* and *Miller* held that, by voluntarily sharing dialed numbers with the phone company and banking records with the bank, consumers waived any right to privacy in those records for purposes of the Fourth Amendment. *Smith*, 442 U.S. at 742; *Miller*, 425 U.S. at 442-43. This so-called "third party doctrine" has, until now, insulated from Fourth Amendment scrutiny the seizure of internet source and destination information from the service providers. *See Forrester*, 512 F.3d at 509-10; *Ulbricht*, 858 F.3d at 96-97. Yet the third party doctrine is at odds with the pervasive use of technology today and the concomitant expectation citizens have that the information they enter into their computers and cell phones is private. *See Jones*, 565 U.S. at 417-18 (Sotomayor, J.); *see also Riley v. California*, 134 S. Ct. 2473, 2490 (2014). For this reason, Supreme Court is poised to re-consider the third party doctrine this coming term. *See Carpenter v. United States*, S.Ct. No. 16-402 (concerning the warrantless search and seizure of records containing cell site location information).

As Justice Sotomayor recognized in *Jones*, our increasing dependence on technology in daily life requires a reevaluation of the question of "privacy" in the context of the Fourth Amendment:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith*, 442 U.S. at 742, 99 S. Ct. 2577; *United States v. Miller*, 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to

> their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

132 S. Ct. at 957 (Sotomayor, J., concurring); *see also* Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. Davis L. Rev. 781, 837 (2008) (arguing that the third-party doctrine is "extremely dangerous in an increasingly technological world" and must be reconsidered in light of actual societal expectations of privacy in digital information).

The Supreme Court has consistently revisited its Fourth Amendment jurisprudence in light of evolving technology. *See Kyllo*, 533 U.S. at 33-34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology"). *Jones* thus recognized that GPS technology was qualitatively different from its physical surveillance counterpart. 132 S. Ct. at 954. *Riley* similarly rejected any comparison between other physical items in an arrestee's possession and his cell phone. *See* 134 S. Ct. at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [previously]").

Here, as in *Jones* and *Riley*, the realities of modern technology preclude the mechanical application of the 35-year-old *Smith* precedent. The Court could not have foreseen that one day the vast majority of Americans would be hooked up to the world wide web, from their homes, and accomplishing everything from banking to ordering groceries, to obtaining health information, reading news, watching TV shows, making political and charitable donations, viewing pornography, and google-mapping the earth. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (U.S. 2017) ("The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow"). It is inconceivable that the Supreme Court in *Smith* and *Miller* intended so far-reaching an abrogation of our Fourth Amendment rights. *See United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578, at *6 (N.D.

Cal. Mar. 2, 2015)("[T]he pen registers employed in 1979 bear little resemblance to their modern day counterparts").

More and more states are rejecting or curtailing *Smith* and recognizing a reasonable expectation of privacy in information revealed to technology companies. *See, e.g., Commonwealth v. Augustine*, 4 N.E.3d 846, 861-62 (Mass. 2014) (rejecting *Smith* and finding reasonable expectation of privacy in cell site location information under state constitution); *State v. Earls*, 70 A.3d 630, 644 (N.J. 2013) (reasonable expectation of privacy in cell site location information); *Tracey v. State* 152 So. 3d 504, 525 (Fla. 2014) (same); 86 Ops. Cal. Atty. Gen. 198 at *3-4 (2003) (information obtained from pen/trap devices protected under state constitution). This is as it should be and as it eventually must be in the federal system. The "Cyber Age is a revolution of historic proportions." *Packingham*, 137 S. Ct. at 1736. It cannot be permitted to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34.

B. THE SURVEILLANCE EXCEEDED STATUTORY AUTHORITY BECAUSE IT REVEALED CONTENT INFORMATION

18 U.S.C. § 3122(a)(1) permits the government to apply for "...an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device." Pen register/trap and trace ("pen/trap") is a "device or process" which "records," "decodes," or "captures" the "dialing, routing, addressing, or signaling information" on outgoing communications or "the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(3)&(4). "[S]uch information shall not include the contents of any communication." 18 U.S.C. § 3127(3)&(4); *see also In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 47 (D. Mass. 2005) ("[T]he government is not entitled to receive '...dialing, routing, addressing, or signaling information ...

reasonably likely to identify the source of a wire or electronic communication" … if [that information]… reveals the 'contents' of a communication"); *United States v. Willard,* No. 3:10-CR-154, 2010 WL 3784944, at *2 (E.D. Va. Sept. 20, 2010) ("When using a pen register or trap and trace device on a computer, the government is not entitled to receive information from the device if that information reveals the contents of a communication"). "'[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication." 18 U.S.C. § 2510(8).

Gottesfeld contends that a continuous tracking of his online activities, in real time, 24 hours a day for 60 days, garners information that constitutes "content." Whereas in the times of telephones, the distinction between numbers dialed and the "content" of a conversation was clear, that line has been blurred by our vast and expanding use of technology. *See In re Application,* 396 F. Supp. 2d at 47-48 (noting the difficulty and considering bank account numbers and search terms to be types of content); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 138 (3d Cir. 2015) ("under the surveillance laws, 'dialing, routing, addressing, and signaling information' may also be 'content'").

The government, in its application, offers this line of demarcation: "the website 'Amazon.com' does not contain the content of any communication, a URL that lists what book the user is searching for on Amazon.com could be considered to contain the content of a communication." Ex. B at 4 n.2; *see also Forrester*, 512 F.3d at 504 n.6 (drawing the same distinction: "a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed").

Yet there is no principled distinction between the two; "content" is a matter of degree. *See Forrester*, 512 F.3d at 510 n. 6 ("[a] URL, unlike an IP address, identifies the particular document

within a website that a person views and thus reveals *much more* information about the person's [i]nternet activity" (emphasis added)). Government surveillance that reveals that a citizen, in his own home, views The New York Times, Amazon.com, WebMd – or Pornhub – reveals a trove of information about his life. That more detailed search information – which book, which kind of pornography – would reveal *more* content does not render the destination information, in the aggregate, mere "means of establishing communication." *Smith*, 442 U.S. at 741; *see Jones*, 132 S. Ct at 956 (Sotomayor, J., concurring) (noting that "the sum of" data points which are innocuous and public, on an atomized level, become meaningful and private when viewed in the aggregate). *But cf. Ulbricht*, 858 F.3d at 96 (affirming the warrantless collection of "IP address information devoid of content"); *Forrester*, 512 F.3d at 510 ("e-mail to/from addresses and IP addresses ...do not necessarily reveal any more about the underlying contents of communication than do phone numbers").

Moreover, the government here has obtained a layer of information beyond simply the IP addresses with whom Gottesfeld communicated. The warrant application avers that Gottesfeld used the VPN network at riseup.net, *see* Ex. A at ¶ 22, and the TOR network, *id.* ¶ 24. Yet the government would have no way to know, from the IP addresses alone, that he was using that particular service at that IP address. It must have received additional routing information, therefore.

Nor do the government's statements, in the application and proposed order, that it "does not seek the URL for websites visited by the designated account, as this URL could contain content," Ex. B at 1, 4, adequately ensure that the service provider did not simply turn over all of the information, rather than sifting through to discard any content-revealing information. More is required:

> [A] mere statement in an order authorizing the installation of a pen register and/or a trap and trace device that the internet service provider is to disclose only "dialing, routing, addressing and signaling information" and not to reveal "contents" and, in addition, not to

> disclose "dialing, routing, addressing and signaling information" which contains "contents" is insufficient notice to the internet service provider as to what may and may not be disclosed. Accordingly, in my judgment, an order to an internet service provider should contain a listing, to the extent possible, of what may NOT be disclosed pursuant to the order.

In re Application, 396 F. Supp. 2d at 49 (D. Mass. 2005).

No such safeguards were provided here. *See id.* ("to impose upon the internet service providers the necessity of making sure that they configure their software in such a manner as to disclose only that which has been authorized, the Court will include a provision to the effect that a violation of the order, including the disclosure of prohibited information, may be found to be a contempt of Court and subject the violator to punishment); *see also In Matter of Application of U.S. For an Order Authorizing the Installation & Use of a Pen Register & a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 18 (D.D.C. 2006) (noting that "some caution… is warranted to make certain the court order clearly identifies what is permitted and, more importantly, what is prohibited so there is no question about the scope of the authorized activities," and finding this caution was exercised when the application and proposed order "explicitly identif[ied] the information the process or device [wa]s intended to collect and noticeably omit[ted] content from the request").

Suppression should be the remedy for a violation of the pen/trap statute. It is the only avenue available to vindicate the rights at issue. *See Hudson v. Michigan*, 547 U.S. 586, 126 S.Ct. 2159, 2163, 165 L.Ed.2d 56 (2006) ("Suppression of evidence ...has always been our last resort"). *But cf. United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir.1995) ("[T]he statutory scheme [of the pen register statute] does not mandate exclusion of evidence for violations of the statutory requirements."); *United States v. Thompson*, 936 F.2d 1249, 1249–50 (11th Cir.1991).

C. THE SURVEILLANCE VIOLATED THE STORED COMMUNICATIONS ACT BECAUSE THE GOVERNMENT DID NOT SHOW ARTICULABLE FACTS

The Stored Communications Act, 18 U.S.C. § 2703(d), permits courts to order a third-party communications provider to turn over records when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." *Id.* Here, the government failed to provide "specific and articulable facts" suggesting that Gottesfeld's internet traffic from three months after the DDOS attack would be relevant, in any way, to its investigation.[4] To the contrary. The application states that the DDOS attack happened. Ex. B. at ¶ 15. Records for the account that posted the Youtube video directed towards Boston Children's Hospital gave an IP address to which Gottesfeld was linked. *Id.* at ¶¶ 16-17. From those two pieces of information, the government concludes that "a computer, tablet, smartphone, or other internet-enabled device" at Gottesfeld's house was used to post the Youtube video. *Id.* at ¶ 18. This fails entirely to suggest any relevance for surveillance of Gottesfeld's internet traffic from July to September of 2014. *See* Ex. B at 5 (requesting real-time information for his online activities "continuously, 24 hours per day," on July 17, 2014). Thus, the order violates the Stored Communications Act. For the reasons stated above, suppression is an appropriate remedy.

D. THE REAL-TIME COLLECTION OF CONTENT INFORMATION VIOLATED THE WIRETAP ACT

In order to intercept the *content* of any electronic communication, the government needs a wiretap order. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 136 & nn.31-32 (3d Cir. 2015) (explaining that "Whereas the Wiretap Act governs the interception of communications 'content[ ],' the separate federal Pen Register Act governs the acquisition of non-

[4] The attack took place on April 20, 2014. The government requested 60 days of surveillance beginning July 17, 2014.

content 'dialing, routing, addressing, [or] signaling information."); 18 U.S.C. § 2510(4) (defining "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device"). To obtain a wiretap order, the government must show probable cause and necessity. *See* § 2518(1)(c); *United States v. Williams*, 524 F. App'x 195, 200 (6th Cir. 2013).

Because the information the government obtained in this case was content information, rather than purely "means of communication," *see In re* Google, 806 F.3d at 136, its real-time surveillance of Gottesfeld violated the Wiretap Act. The evidence should be suppressed on this basis as well.

II. ABSENT THE ILLEGALLY OBTAINED INFORMATION, THE WARRANT CANNOT STAND

The information contained in the search warrant affidavit that was obtained in violation of Gottesfeld's Fourth Amendment rights, namely ¶¶21-26, must be excised from the affidavit for purposes of determining whether probable cause existed to justify issuance of the warrant. *See United States v. Asaro*, 2014 U.S. Dist. LEXIS 84171, *9, No. 12-10196-GAO (D. Mass. June 20, 2014) (writing that when evidence that was obtained in violation of constitutional rights is included in warrant application, suppression is warranted "only if, the 'offending information' being ignored, what remained in the affidavit was insufficient to establish probable cause") (citing *United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005); *accord United States v. Zhen Zhou Wu*, 2010 U.S. Dist. LEXIS 4439 (D. Mass. Jan. 21, 2010)). In this particular case, the Court should excise from the affidavit the fact that Gottesfeld used a VPN service through the website www.riseup.net, as well as the fact that he used the TOR network, both services used by individuals seeking to browse the internet anonymously.

Putting aside the unlawfully obtained information about Gottesfeld's internet activity, the affidavit fails to establish probable cause that evidence of a crime would be found at that location. The government had evidence that Gottesfeld was the one who posted the Anonymous video on YouTube almost a month before the DDOS attack on Children's Hospital. However, they have no information about where the DDOS attack came from. In fact, they admit as such in their search warrant application: "I have reviewed BCH webserver logs from the time of the DDOS attack. These logs showed hundreds of IP addresses flooding the BCH network with malicious traffic. The IP addresses sending this malicious traffic resolve to geographically dispersed locations." Ex. A. at ¶15.

Without the information regarding Gottesfeld's use of riseup.net's VPN service and the TOR network, the affiant would not be able to give his opinion that these services are often used by criminals "in an effort to evade law enforcement." Ex. A. at ¶26. The affiant also would not be able to link Gottesfeld in any way to two Twitter accounts, @AnonMercurial and @PacketSignal, which tweeted about the Children's Hospital DDOS attack using TOR and riseup.net IP addresses. *Id.* at ¶25.

What the government is left with when the internet traffic information is excised is that Gottesfeld posted the YouTube video about a month before the attack, as well as that Gottesfeld is an activist against the "troubled teen industry" and had been outspoken against two other organizations that experienced DDOS attacks. Ex. A. at ¶¶27-31. Those facts, however, do not establish probable cause to believe that Gottesfeld committed those DDOS attacks, or that evidence of any crime would be found at his apartment.

III. THE SEARCH WARRANT IS UNCONSTITUTIONALLY OVERBROAD

Given the pervasive and personal nature of technology, warrants must be tailored to seize only those devices that are (a) connected to the person being targeted and (b) connected to the

crime. Here, the warrant gave the government blanket permission to seize "[a]ll computer hardware," and "any computer hardware (including smartphones and tablets), computer software, or storage media ...." Attachment B (Items to be Seized) to Search Warrant (here, Ex. A) at ¶ I.D, ¶ II. It is in no way tailored to the type of device suspected – or even capable – of causing the DDOS attack. Furthermore, the warrant goes beyond seizing devices of Gottesfeld's. It gives the government permission to seize literally "any" computer, phone, tablet, "or storage media" that is at the house. Indeed, the affidavit affirmatively *requests* permission to "search and seize... on-site or off-site ..., regardless of how their contents or ownership appear or are described by others at the scene of the search." Ex. A ¶ 35. It fails to justify why it needs unfettered access to *anyone*'s devices, *of any kind*, that may happen to be at that address on that day. Such a warrant has been held to be unconstitutionally overbroad. *See United States v. Griffith*, No. 13-3061, 2017 WL 3568288, at *7 (D.C. Cir. Aug. 18, 2017) (finding search warrant for the seizure "of all electronic devices found in the residence," a year after a gang-related homicide, was unconstitutionally overbroad). Furthermore, the warrant granted permission not only to seize the items, but to search them as well. *See United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (noting the "private information individuals store on digital devices—their personal 'papers' in the words of the Constitution"); *cf. Griffith*, No. 13-3061, 2017 WL 3568288, at *16 (Brown, J., dissenting) (noting that the warrant in that case "only authorized the *seizure* of the electronic devices, not a *search* of their content" (emphasis in original). Because the search warrants fails to describe with any particularity the things to be seized, the warrant issued in violation of the Fourth Amendment's requirement that warrants "particularly describ[e]" the "things to be seized." The warrant is therefore invalid and evidence obtained pursuant to the execution of this warrant must be suppressed.

CONCLUSION

For the reasons set forth above, the search warrant in this case cannot stand. The Court should suppress any items seized from the house and any information obtained as a result of those items.

MARTIN GOTTESFELD,
By His Attorneys,

/s/ Jane F. Peachy
Jane F. Peachy, BBO#661394

/s/ Amy Barsky
Cal. Bar 270846

Federal Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Jane F. Peachy, Esquire, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on August 31, 2017.

/s/ Jane F. Peachy
Jane F. Peachy

Exhibit N

Trump Should Be Wary Of This Would-Be Ally Too

DIARY / MARTY GOTTESFELD // Posted at 11:49 am on September 16, 2017 by Marty Gottesfeld

Martin Gottesfeld was featured by Michelle Malkin for defending Justina Pelletier when she was maimed at Harvard-affiliated Boston Children's Hospital, leading to his imprisonment without bail by a Harvard-affiliated judge and Obama-appointed prosecutors at the Plymouth County Correctional Facility (PCCF). See FreeMartyG.com for more info and social media links.

When President Trump announced his first immigration actions, liberal cities and towns immediately started resisting. Some passed ordinances declaring themselves sanctuaries for immigrants while their state legislators and courts went to work on supporting statutes and case law. As one of the bluest members of the union, Massachusetts is in the process of declaring itself a "sanctuary state," and as one of the only two county sheriffs therein to agree to cooperate with federal immigration authorities, Joseph McDonald Jr. has received praise from a variety of conservative outlets.

Joseph McDonald Jr., the Sheriff of Plymouth County, Massachusetts, has been cozying up to the Trump administration via its immigration policies, but the president should be careful about embracing him. Photo courtesy of Massachusetts Sheriffs' Association.

TRENDING

1 *SCANDAL. Donald Trump Is Handicapping Supreme Court Vacancies*

2 *Paul Ryan Blows Off Bannon's Declaration of "War"*

3 *Hillary Clinton Is Nearly Right About This One Thing*

4 *Trump's Cheap "Merry Christmas" Christianity Continues to Sway Evangelicals*

5 *Jimmy Kimmel Does Not Want to Talk to You*

SCANDAL. Donald Trump Is Handicapping Supreme Court Vacancies

streiff

Kaepernick to NFL Owners: You've Colluded Against Me!

Susan Wright

Jimmy Kimmel Does Not Want to Talk to You

Patterico

While superficially Sheriff McDonald's motives seem ideological, further inspection reveals more sinister intentions seemingly at play and McDonald's checkered past makes him a liability for would-be political allies, especially an administration under scrutiny from liberal media outlets with their fangs out as well as human rights and immigrants' groups looking for egregious abuses on which to hang their hats. McDonald could also find himself under fire for his mistreatment of U.S. combat veterans, a group important to Trump, who endure the same tortures as the federal immigration detainees in McDonald's custody at the Plymouth County Correctional Facility (PCCF).

For example, a marine I'll call "N," who's currently being held on a bogus Massachusetts gun charge at PCCF, has claustrophobia and Post-Traumatic Stress Disorder (PTSD) from when his Humvee was flipped by an IED and his team was pinned inside by enemy gunfire. Despite being told of N's diagnosis, as well as previous articles about PCCF's prior mistreatment of veterans at The Huffington Post and ShadowProof, management tried to move him from an open dormitory unit to a small cell – twice.

The first time, N said he could not enter the small cell. PCCF management retaliated by placing him on suicide watch and forcing him into the jail's Q5 unit. There, N says he spent the night unable to sleep, nearly naked in a tiny approximately 40-degree Fahrenheit cell without a mattress or blanket.

Dozens of others tell similar stories of Q5, where they say skin turns purple and sticks to the cold floor like the cliché tongue on a frozen flagpole. One reported dead flies on the floor and another described seeing a previous occupants' pubic hair strewn about. The first thing many want to tell the public is that one of the cells in Q5 has no toilet — instead they describe having to defecate in a hole in the ground.

After being cleared off suicide watch by mental health staff the next morning and returning to the open dorm, N said his night in Q5 was the worst experience of his life – worse than being pinned down inside the Humvee. He marveled at the probable media backlash if U.S. troops put enemy POWs through such treatment.

Two days later they tell N they're moving him to a cell again. A guard who happens to be a fellow combat vet makes calls on N's behalf, to no avail. Given the choice between a small cell in Q5 and an equally small but warmer one elsewhere, N goes along and endures the insomnia and nightmares when he eventually passes out from exhaustion. Adding insult to injury, before the second move they lie, telling him he's headed for a newly established veterans' wing, but he soon discovers there's no such thing.

Don't Let Iran Become the Next North Korea

Dan Spencer

FCC Commissioner to Trump: First Amendment, Baby! Learn to Love it!

Susan Wright

Trump's Cheap "Merry Christmas" Christianity Continues to Sway Evangelicals

Kimberly Ross

As for McDonald's seemingly brave choice to back Trump's immigration policies from inside deep blue Massachusetts, PCCF stands to gross over $100/day for each additional immigrant ICE now plans to detain there in an apparent quid pro quo. However, here too the specters of the past and future loom large.

First, it's not hard to imagine an international backlash welling up when ICE detainees abused by PCCF are deported to their home countries and start talking about their experiences. Q5 could constitute torture under U.N. treaties and PCCF has already been featured in a report to the U.N. committee in charge of investigating torture worldwide.

Also, back in February 2015, while ICE was already contracting with PCCF to hold some immigrants, Channel 5 News in Boston aired a story about a PCCF supervisor accused by another jail employee of offering coworkers thousands in cash to marry Vietnamese women in need of U.S. citizenship.

The local news crew found 3 matching marriages and divorces recorded between PCCF guards and Vietnamese immigrants and even found one of the women working at the alleged mastermind's nail salon located down the street from PCCF.

There's newer ground for intrepid Massachusetts reporters to break at PCCF as well. Many current staff say McDonald employs a pay-to-play system and that it's well understood that obtaining coveted promotions requires candidates to donate to the Sheriff's reelection campaign. Indeed, local papers make note of the large amount of campaign contributions McDonald receives from his subordinates, and many of the longest-tenured employees at PCCF say that's not just a result of employees' heartfelt support for McDonald.

Finally, while there are numerous other issues at PCCF which should give the Trump administration pause, no list should go without the elephant in the room — despite this long history, Obama's U.S. Attorney in Boston oddly left McDonald alone for nearly 8 years despite being aware of the 2015 allegations. In contrast, George W. Bush's appointee prosecuted a police sergeant from a town police department in Plymouth County for similar marriage fraud involving German women.

He told the local news crew investigating the allegations of marriage fraud at PCCF, "As a prosecutor I have kind of a heightened interest with regards to any type of law enforcement participating in any type of fraud, including marriage fraud."

https://www.redstate.com/diary/MartyGottesfeld/2017/09/16/trump-wary-ally/ 3/6

Sheriff James DiPaola committed suicide on November 26, 2010 while facing breach of ethics allegations from state authorities and the press.. Photo via middllesexsheriff.org

In further contrast, Obama's federal prosecutors did go after a nearby Democratic former Middlesex County, Massachusetts sheriff James Dipaola. Sheriff DiPaola shot himself in the head as the State Ethics Commission was closing in on him over allegations funds for his re-election were illegally being raised by his employees.

So, why the difference? The public should know, and so should the Trump administration before it jumps into bed with Mr. McDonald.

FEDERAL DEFENDER OFFICE
DISTRICT OF MASSACHUSETTS
51 SLEEPER STREET, FIFTH FLOOR
BOSTON, MASSACHUSETTS 02210

TELEPHONE: 617-223-8061
FAX: 617-223-8080

Exhibit X

September 22, 2017

Martin Gottesfeld
Reg. #12982-104
Plymouth County Correctional Facility
26 Long Pond Road
Plymouth, MA 02360

RE: United States v. Martin Gottesfeld
Criminal No. 16-10305-NMG

Dear Marty:

I received the voicemail you left me this morning about the search of your unit and an officer reading your legal mail. I spoke to general counsel for the Plymouth County Sheriff's Department, and he tells me that the assistant superintendent is reviewing the video of the search of the unit. They said the search was a general search for contraband due to the fact that they were moving some prisoners, but they are investigating now based on your complaint. They said they will let me know what they see on the tape. I will keep you posted.

You said in your voicemail that you wanted me to file something with the court instead of contacting the jail's counsel, but it is my opinion that this was the best way to handle the situation. I do not intend to move to withdraw because I do not see an irretrievable breakdown in communication between us. If you would like new counsel, then you can file a motion with the Court requesting same.

Sincerely,

/s/ Jane F. Peachy
Jane F. Peachy
Assistant Federal Defender

JFP/ac

Exhibit Y

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	No.: 16-cr-10305-NMG
	)	
MARTIN GOTTESFELD,	)	
	)	
Defendant.	)	

GOVERNMENT'S OPPOSITION
TO DEFENDANT GOTTESFELD'S MOTION TO SUPPRESS EVIDENCE

The United States of America, by Assistant United States Attorneys David J. D'Addio and Adam J. Bookbinder, hereby submits this response in opposition to Defendant Martin Gottesfeld's Motion to Suppress Evidence (Dkt. No. 78).

I. INTRODUCTION

Defendant Gottesfeld seeks to suppress evidence obtained from execution of a search warrant at his Somerville apartment on October 1, 2014. He challenges the warrant on two grounds: (1) first, he claims that information obtained from a court-authorized pen register and trap and trace was essential to the probable cause showing and was obtained in violation of the Fourth Amendment and various statutes; (2) second, he claims that the warrant was not sufficiently particular. Both claims are without merit.

As set forth below, the government obtained a Court order to install a pen register and trap and trace ("PRTT") device on the internet service account for the defendant's former residence on July 17, 2014. The PRTT collected non-content routing information—specifically dates, times, IP addresses, and communication ports—for internet activity to and from the internet account servicing that address—28 Albion Street, Apartment 1 in Somerville, Mass.

The court's order and the execution of that order by law enforcement complied fully with the authorizing statute, 18 U.S.C. § 3121-27 (the "Pen/Trap Act"). Defendant nonetheless contends that collecting the specific information authorized by both the Pen/Trap Act and the court order violated his Fourth Amendment rights—a conclusion rejected by every federal court to consider the question, including the Eight Circuit and, this spring, the Second Circuit. The reasoning of these of decisions—unchallenged by the defendant in any meaningful way—is persuasive, is grounded in long-standing Supreme Court precedent, and should be adopted by this Court. Even if this Court were to be the first in the nation to declare the Pen/Trap Act unconstitutional, however, the evidence still should not be suppressed because law enforcement acted reasonably and in good faith when it relied on the Pen/Trap Act and the court's order authorizing installation of a PRTT device to obtain the non-content routing information at issue. Suppression of evidence—a remedy of last resort under the Fourth Amendment—is inappropriate under these circumstances. Moreover, even without the PRTT data, the search warrant affidavit still established probable cause to search the defendant's apartment.

As to the warrant's particularity, the supporting affidavit set forth probable cause to believe that the specific location, and the electronic devices in that location, would constitute or contain evidence of violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 and the federal conspiracy statute, 18 U.S.C. § 371. The attachments to the warrant set forth these statutory violations and further provided specific examples of the types of documents and information to be seized. In short, there are no grounds to suppress the evidence obtained from the October 1, 2014 search. For these reasons, defendant's motion should be denied.

II. BACKGROUND

A. The Pen/Trap Act Authorizes Prospective Collection of Addressing and Routing Information, Such as IP Addresses, for 60 Days.

The Pen/Trap Act authorizes installation of a "pen register" to record or capture, prospectively, "dialing, routing, addressing, or signaling information" that is "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). The Pen/Trap Act prohibits collection of "the contents of any communication," *id.*, thus drawing a distinction between the non-content information necessary to route a communication from its source to its destination, and the content of the communication itself.

Similarly, the Pen-Trap Act authorizes installation of a "trap and trace" device to "identify the originating number or . . . source of a wire or electronic communication," 18 U.S.C. § 3127(4). Like the pen register provision, the trap and trace provision prohibits collection of "the contents of any communication." *Id.* To install either device, the government must certify that the information likely to be collected is "relevant to an ongoing criminal investigation" but it is not required to establish probable cause or obtain a warrant. 18 U.S.C. § 3122.

Congress amended the Pen/Trap Act in 2001 explicitly to include non-content addressing information for internet communications, in addition to telephone toll records. USA Patriot Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288 (2001); 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (describing amendment as a way to "ensure[ ] that the pen register and trap and trace provisions apply to facilities other than telephone lines (e.g., the Internet)"); 147 Cong. Rec. S11,049 (daily ed. Oct. 25, 2001) (statement of Sen. Kyl) (noting that language ultimately adopted "would codify current case law that holds that pen/trap orders apply to modern communication technologies such as e-mail and the Internet, in addition to traditional phone lines."); 147 Cong. Rec. H7,197 (daily ed. Oct. 23, 2001) (statement of Rep.

Conyers) (describing amendment as extending "the pen/trap provisions so they apply not just to telephone communications but also to Internet traffic, so long as they exclude 'content.'"). *See generally In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of A Pen Register and a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 16-17 (D.D.C 2006) (discussing text and legislative history of Pen/Trap Act and concluding: "The plain language of the statute makes clear that pen registers and trap and trace devices may be processes used to obtain [routing] information about e-mail communications. The statute's history confirms this interpretation and there is no support for a contrary result.")

B. The Government Obtained Authorization to Install a PRTT Device to Capture Source and Destination IP Addresses For Internet Traffic Over Defendant's Internet Service Account.

On July 17, 2014, the government applied for an order seeking authorization under the Pen/Trap Act to install, for 60 days, a pen register and trap and trace device "to trace the source and destination of all electronic communication directed to or originating from" the RCN Telecom Services LLC ("RCN") account providing internet service to 28 Albion Street, Apt. 1, in Somerville—the Defendant's prior address—along with the date, time, size, and duration of these communications. Dkt. No 78, Ex. C at 4. The application expressly stated the "United States does not seek 'content,' in any form, of any electronic communication." The application further provided that the government "does not seek the URL for websites visited by the designated account, as this URL could contain content." *Id.* Regarding the types of non-content routing information at issue, the application explained:

> Data packets transmitted over the internet—the mechanisms for all internet communications—contain addressing and routing information analogous to the destination phone numbers captured by traditional pen registers and the origination phone numbers captured by traditional trap and trace devices. One example of this addressing and routing information is an IP address, which is a unique numeric address used by computers on the internet. Another example of this addressing and routing information is a "port,"

> which is a numeric identifier of a particular type of service being offered by a computer or server. For example, port 80 is typically reserved for World Wide Web traffic, so that a computer that wishes to retrieve information from a web server would typically connect to port 80.

Id. at 2.

On July 17, 2014, U.S. Magistrate Judge Jennifer C. Boal issued an order authorizing law enforcement to install a pen register/trap and trace device to capture, for 60 days, "the source and destination IP address and port of all electronic communications," along with the date and time of those communications, to or from the defendant's internet service account with RCN.[1] Dkt. No. 78, Ex. C. at 2. An example of the data provided to the FBI via the PRTT device is provided in the table below:

Start Date (UTC)	Source IP	Source Port	Destination IP	Destination Port
8/9/2014 11:48 AM	209.6.193.140	1534	50.57.60.203	161
8/9/2014 11:48 AM	209.6.193.140	1536	50.57.60.203	161
8/9/2014 11:47 AM	209.6.193.140	1541	50.57.60.203	161

RCN provided no additional types of information (*e.g.*, file size, duration of communication, or any manner of content). The government produced the data provided by RCN to defense counsel in discovery.

C. The Government Obtained a Warrant to Search Defendant's Residence.

On September 30, 2014, the Honorable Marianne B. Bowler issued a warrant to search defendant's residence, at 28 Albion Street, Apartment 1, in Somerville, Mass. The warrant application incorporated a supporting affidavit that described the distributed denial of service perpetrated against the computer network of the Boston Children's Hospital, along with an array of evidence linking Gottesfeld to that cyberattack as well as attacks on other entities Gottesfeld

[1] The order further authorized collection of the "size" of the communications and their duration—neither of which constitutes the content of the communications. However, this information was not provided by RCN.

campaigned against. The warrant authorized agents to search for and seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(5)(A) (intentionally causing damage to a protected computer) and 18 U.S.C. § 371 (conspiracy). More specifically, the warrant set forth a list enumerating, among other things, specific people, entities, IP addresses, websites, social media accounts, and topics relating to the Children's Hospital DDOS attack and other entities targeted by Gottesfeld and/or the hacking collective known as "Anonymous," for which the warrant authorized the search. Agents executed the warrant on October 1, 2014, seizing multiple electronic devices containing evidence of Gottesfeld's involvement in the attack on the Boston Children's Hospital.

After the search, Gottesfeld retained counsel and began discussions with the U.S. Attorney's Office about a possible pre-indictment plea. But on February 16, 2016, after the government learned that Gottesfeld and his wife had fled the country in a small boat, the U.S. Attorney charged him, by criminal complaint, with conspiracy (18 U.S.C. § 371) to intentionally cause damage to protected computers (18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B)). Gottesfeld was arrested in Miami on February 17, 2016. He was indicted, on October 19, 2016, on one count each of conspiracy and damaging protected computers.

III. ARGUMENT

A. Collection of IP Addresses Is Not a Search Under the Fourth Amendment

The Supreme Court has held, in the context of telephones, that the use of a pen register does not constitute a "search" under the Fourth Amendment, for which a warrant is required, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," such as the dialing instructions he conveys to telephone companies when he makes a call. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). *See also United States v. Miller*, 425 U.S. 435 (1976) (no expectation of privacy in information voluntarily turned over to

banks as reflected in banking records). This same principle behind the "third party doctrine" applies when a pen register is used to collect data, such as IP addresses, that is used to route electronic communications over the internet—a circumstance that is "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).

Just like telephone users, internet users "rely on third-party equipment in order to engage in communication" and "have no expectation of privacy in . . . the IP addresses of the websites they visit, because they should know that this information is provided to and used by internet service providers for the specific purpose of directing the routing of information." *Forrester*, 512 F.3d at 510; *accord United States v. Ulbricht*, 858 F.3d 71, 96 (2d Cir. 2017). Indeed, "IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over to direct the third party's servers." *Ulbricht*, 858 F.3d at 96 (quoting *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010)).

Earlier this year, in *Ulbricht*, the Second Circuit squarely rejected a Fourth Amendment challenge to the Pen/Trap Act that mirrored that brought by defendant Gottesfeld. *Ulbricht*, 858 F.3d at 96. Addressing the collection of the same IP routing information at issue here, the Second Circuit concluded:

> The recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in *Smith*. . . . The substitution of electronic methods of communication for telephone calls does not alone create a reasonable expectation of privacy in the identities of devices with whom one communicates. Nor does it raise novel issues distinct from those long since resolved in the context of telephone communication, with which society has lived for the nearly forty years since *Smith* was decided. Like telephone companies, Internet service providers require that identifying information be disclosed in order to make

> communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information.

Ulbricht, 858 F.3d at 97.

Accordingly, IP addresses and similar internet routing information are not protected by the Fourth Amendment and can be collected without a warrant under the Pen/Trap Act. *See Ulbricht*, 858 F.3d at 97 (joining other circuits and holding that "collecting IP address information devoid of content is 'constitutionally indistinguishable'" from the use of a telephone pen register) (quoting *Forrester*, 512 F.3d at 510). *See also United States v. Graham*, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (noting that "third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection"); *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016) ("[C]ourts have not (yet at least) extended [Fourth Amendment] protections to the internet analogue of envelope markings, namely the metadata used to route internet communications like . . . IP addresses"). *See generally In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of A Pen Register and a Trap & Trace Device on E-Mail Account*, 416 F. Supp. 2d 13, 16-17 (D.D.C 2006) (applying Pen/Trap Act to email accounts where government "explicitly identif[ied] the information" the PRTT was to collect and omitted "content" of the communications); *In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (Collings, J.) (finding with regard to an internet PRTT application that: "If, indeed, the government is seeking only IP addresses of the web sites visited and nothing more, there is no problem").

Recognizing that the third-party doctrine is fatal to his claim, defendant invites this Court to disregard it, arguing that the third-party doctrine is "at odds with the pervasive use of technology today" and noting that the "Supreme Court is poised to revisit the third party doctrine," which the Defendant concedes has "heretofore insulated this information from Fourth Amendment protection." Dkt. No. 78 at 4. Defendant argues that if he is liberated from this precedent, then IP addresses for his internet activity, when aggregated over the 60-day period authorized by the Pen/Trap Act, constitute information in which he has a reasonable expectation of privacy under *Katz v United States*, 389 U.S. 437 (1967). Dkt. 78 at 5-6. In the alternative, he claims that IP addresses themselves constitute the *content of his communications*, and therefore obtaining such routing information without a warrant violated the Fourth Amendment, as well as the Pen/Trap Act and the Wiretap Act, 18 U.S.C. §§ 2510-22. As is discussed below, these arguments are meritless.

B. Defendant Has No Reasonable Expectation of Privacy in Routing Data Obtained Under the Pen/Trap Act.

The Fourth Amendment's prohibition on unreasonable searches was originally understood to be "tied to common-law trespass." *United States v. Jones*, 565 U.S. 400, 405 (2012). Since the Supreme Court's decision in *Katz*, however, a Fourth Amendment search may also "occur[] when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001). The First Circuit has accordingly stated, "The Supreme Court set out a two-part test for analyzing the expectation [of privacy] question: first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation [of privacy] is one that society is prepared to recognize as objectively reasonable." *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) (citing *Smith*, 442 U.S. at 740).

i. Defendant Has Failed To Assert a Subjective Expectation of Privacy in the Source and Destination IP Addresses of his Internet Communications.

Establishing a reasonable expectation of privacy is the defendant's burden. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980); *United States v. Lewis*, 40 F.3d 1325, 1333 (1st Cir. 1994). When a defendant fails to provide an affidavit in support of a motion to suppress, "it is almost impossible to find a privacy interest because this interest depends, in part, on the defendant's subjective intent and his actions that manifest that intent." *United States v. Ruth*, 65 F.3d 599, 604-05 (7th Cir. 1995). Here, Defendant has failed to file an affidavit in support of his motion, which rests only on the limited, conclusory statements of his lawyers regarding his expectation of privacy in his own IP address and those of the servers with which he communicated via the internet. The only suggestion that the defendant actually believed that the routing information for his internet activity was private is his lawyers' assertion that the defendant "used encryption services—the only way an individual can attempt to hold onto his privacy while using the internet." Dkt. No. 78 at 7. Far from establishing a subjective expectation of privacy, defendant's use of anonymizing technologies suggests the opposite—that he knew that routing information regarding his internet traffic was not private, but instead was available to his internet service provider and servers he communicated with, as this information must be conveyed in order for internet traffic to flow. Thus, he used various encryption services to attempt to limit his public exposure. Because the defendant has failed to assert a subjective privacy interest in the routing information at issue, the Court may deny the defendant's motion to suppress without a hearing. *See United States v. Lewis*, 40 F.3d 1325, 1333 (1st Cir. 1994).

ii. Any Subjective Expectation of Privacy in IP Routing Information Is Objectively Unreasonable.

Even if Defendant were to establish that he personally expected the non-content routing information for his internet traffic would be private, such an expectation is not one that society

recognizes as reasonable. "Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information." *Ulbricht*, 858 F.3d at 97. This basic proposition, built upon binding Supreme Court precedent, is further buttressed in this case by Congress's decision to expressly incorporate the *Smith* rule when it expanded the Pen/Trap Act to cover internet communications. *See supra* Part II.A.[2] Although this defendant claims that real-time collection of internet routing information, "for 60 days, goes well beyond what ordinary people expect the government to be observing," Dkt. No. 78, that this is precisely what the "ordinary people's" elected representatives authorized the government to collect in passing the 2001 amendments to the Pen/Trap Act.[3]

Defendant recognizes that the "third-party doctrine" has to date precluded any Fourth Amendment claim where the government compels disclosure of records voluntarily provided to a third party, including the records for routing internet traffic at issue here. Dkt. No. 78 at 8. He nonetheless contends that the third-party doctrine is inconsistent with the widespread use of modern technology, relying principally on Justice Sotomayor's concurrence in *Jones*, 565 U.S. at 414 and the majority opinion in *Riley v. California*, 134 S. Ct. 2473 (2014). Dkt. No. 78 at 8-9. He further notes that some states have limited the application of the third-party doctrine to

---

[2] As the House of Representatives noted in its report regarding the enactment of the PATRIOT Act, "the statutorily prescribed line between a communication's contents and non-content information" is "identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741–43 (1979)." H.R. Rep. No. 107–236, at 53 (Oct. 11, 2011).

[3] This point is a crucial one and distinguishes the instant case from *Jones*, in which law enforcement used GPS devices to track the suspect's precise location for 28 days, 565 U.S. at 402-03, without any express authorization by a court or Congress.

certain technologies under state law, and that the Supreme Court is "poised to reconsider the third party doctrine this coming term." *Id.* at 8, 10.

Whatever the Supreme Court might decide in the future with respect to the third-party doctrine, this Court remains bound by the holdings of *Smith* and *Miller* unless and until the Supreme Court overrules them. *See United States v. Ivery*, 427 F.3d 69, 75 (1st Cir. 2005) ("It is not our place to anticipate the Supreme Court's reconsideration of its prior rulings"). Indeed, the Supreme Court "has admonished the lower federal courts to follow its directly applicable precedent, even if that precedent appears weakened by pronouncements in its subsequent decisions, and to leave to the [Supreme] Court 'the prerogative of overruling its own decisions.'" *Figueroa v. Rivera*, 147 F.3d 77, 81 n.3 (1st Cir. 1998) (quoting *Agostini v. Felton*, 521 U.S. 203, 237 (1997). *See also Ulbricht*, 858 F.3d at 96-97 (rejecting Ulbricht's call to re-evaluate the *Smith* doctrine in light of "great quantities of personal information" provided to third parties).

In any event, Defendant's reliance on *Jones* and *Riley* to sidestep the third-party doctrine is misplaced. *Jones* and *Riley* did not address—much less disavow—the Supreme Court's precedents recognizing that an individual does not have a Fourth Amendment interest in a third party's records pertaining to him or in information that he voluntarily conveys to third parties. Because the Court in *Jones* concluded that the attachment of a GPS device constituted "a classic trespassory search," 565 U.S. at 412, it did not reach the *Katz* inquiry.[4] *Riley* is even further afield. *Riley* held that a law-enforcement officer generally must obtain a warrant to search the

[4] Defendant cites *dicta* addressing *Katz* in a wholly distinct context: aggregation of 28 days of data obtained from law enforcement's covert installation and use of GPS tracking device without a warrant, court order, or any express statutory authorization. Here, in contrast, the government used compulsory process in the form of a court order expressly authorized by statute to obtain records of information the defendant' voluntarily turned over to a third party—his internet service provider.

contents of a cell phone found on an arrestee. 134 S. Ct. at 2485. No question existed in *Riley* that the review of the contents of a cell phone constitutes a Fourth Amendment search; the question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. *See id.* at 2482 ("The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest."); *see also id.* at 2489 n.1 (noting that "[b]ecause the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances"). Neither *Jones* nor *Riley* presented an occasion for the Supreme Court to reconsider its longstanding view that an individual has no Fourth Amendment interest in records pertaining to an individual that are created by third parties or in information he voluntarily conveys to third parties. Nor do these cases provide any grounds for this Court to otherwise distinguish *Smith* and *Miller* in the context of internet routing data.

Likewise, defendant's citations to state law (almost all of which deal with legally distinct concepts and a separate statutory scheme for obtaining historical cell phone location data) are misplaced. The Supreme Court has repeatedly rejected the "suggestion that concepts of privacy under the law of each State are to determine the reach of the Fourth Amendment." *California v. Greenwood*, 486 U.S. 35, 44 (1988). Rather, "when States go above the Fourth Amendment minimum, the Constitution's protections concerning search and seizure remain the same." *Virginia v. Moore*, 553 U.S. 164, 173 (2008). In any case, the enactment of state laws addressing business records such as cell site location records and pen register data confirms that legislatures are best positioned to balance privacy interests and law enforcement needs in light of new

technologies, just as Congress has already done with the Pen/Trap Act. *See Jones*, 565 U.S. at 429-30 (Alito, J. concurring in the judgment).

In short, *Smith* and *Miller* remain controlling law; Congress adopted a statute incorporating those holdings and expressly authorizing law enforcement to collect the internet routing data at issue in this case; and agents followed the statutory procedure in obtaining and executing a court order to collect that information. *See Ulbricht* 858 F.3d at 96-97; *Forrester* 512 F.3d at 510. Accordingly, no Fourth Amendment search occurred, and defendant's motion should be denied.

C. The Internet Routing Information Collected by the Government Is Not "Content."

Defendant "contends that continuous tracking of his online activities, in real time, 24 hours a day for 60 days, garners information that constitutes 'content,'" Dkt. No. 78 at 11, and that accordingly, acquisition of IP addresses via the PRTT violated not only the PRTT, but the Wiretap Act and the Fourth Amendment.

Defendant's argument falters at the first step. As discussed in Part II.A, *supra,* the Pen/Trap Act authorizes collection of "dialing, routing, addressing, or signaling information," but prohibits collection of "the contents of any communication." There is no question that the "dialing, routing, address, or signaling information" includes source and destination IP addresses for internet communications. *See* Part II.A, *supra*. By defining aggregated IP addresses as "content," defendant renders the Pen/Trap Act a nullity for the very types of communications it was intended to cover—*i.e.*, the Pen/Trap Act cannot authorize the collection of IP addresses while *simultaneously prohibiting* the collection of those same IP addresses. Such a reading of the Pen/Trap Act is nonsensical, is untethered from any authority cited by the defendant, and should be rejected out of hand by this Court.

Defendant goes on, however, to offer hypothetical circumstances in which information that might be considered routing information, may also convey the "the substance, purport, or meaning of that communication," 18 U.S.C. § 2510(8), and thus constitute "content" within the meaning of the Pen/Trap Act, 18 U.S.C. § 3127(1) and the Wiretap Act. Oft-cited examples include, in the context of telephone calls, so-called "post-cut-through digits," (*i.e.*, numbers dialed after the initial call is placed or "cut through"), and in the context of internet traffic, website Uniform Resource Locators ("URLs") that can contain information such as search terms entered or specific web pages visited. *See generally, In re Google, Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 128, 135-39 (3d Cir. 2015); *In re Application of U.S. for an Order Authorizing use of A Pen Register & Trap On (XXX) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 47-69 (D. Mass. 2005) (Collings, J.).

None of these concerns are present in this case, where the routing information consisted solely of IP addresses, communication ports, dates, and times. Just as no court has ever held that the initial telephone number dialed (or incoming number received) constitutes the "contents" of a telephone communication, no court has ever held that an incoming or outgoing IP address constitutes the "contents" of an electronic communication made via the internet. Every relevant case cited by the defendant either holds or assumes the same. The Court therefore stands on firm ground in rejecting the claim actually made by the defendant—that IP addresses can constitute communicative content as opposed to routing information—and deferring judgment on his discussion regarding when other types of routing information not relevant to this case may simultaneously constitute communicative "content." *See Ulbricht*, 858 F.3d at 98 n.29 (confining its opinion to "the capture of IP addressed, TCP connection data, and similar routing information" under the Pen/Trap Act), *Forrester*, 512 F.3d at 510-11, 511 n.6 (noting that

surveillance techniques that collect URLs "might be more constitutionally problematic" and limiting its holding to IP addresses and email to/from addresses).

Defendant's claim that the government "has obtained a layer of information beyond simply the IP addresses with whom Gottesfeld communicated" is wrong. The government produced to defendant the PRTT data—it consists solely of dates, times, source and destination IP addresses, and source and destination ports. Defendant is correct that the warrant application states the affiant's belief, based on those IP addresses, that the defendant used the VPN network riseup.net, and the TOR network. As defendant well knows, however, the registration of IP addresses is a matter of public record, and TOR network nodes are also publicly listed. Just as a PRTT on a phone reveals dialed numbers that law enforcement can look up, a PRTT on an internet account reveals IP addresses that law enforcement can look up. In this case, a simple internet query reveals that certain IP addresses with which defendant communicated belonged to particular internet services, including Riseup.net and TOR.

Finally, defendant quibbles with the form of the court's PRTT order, claiming it was inadequate because it did not offer what the defendant believes were sufficient assurances that RCN would not provide information outside the scope of the statutory authorization. Dkt. No.78 at 12-13. The proper measure of the Order, however, is the statute under which it was promulgated, not the defendant's view of best practices. The Order clearly stated that the PRTT device was to provide the "source and destination IP address and port of all electronic communications directed to or originating from the designated account, and to record the date, time, size, and duration of these communications. . . . *RCN shall not provide to the FBI, the URL for websites visited by the designated account.*" Dkt. No. 78, Ex. C at 2 (emphasis added). In short, the court ordered RCN to provide limited, specifically enumerated categories of

information authorized by the statute, and expressly instructed RCN not to provide URLs that, although used for routing, could constitute "content" in certain circumstances. Most important, RCN in fact provided only the dates, times, and source and destination IP addresses and ports—nothing more. There is simply no information RCN provided that could constitute content under any definition in the relevant statutes or case law, and defendant, despite having the actual data, has pointed to none.

D. Law Enforcement Was Entitled To Rely On A Presumptively Constitutional Statute and a Duly Executed Order of the Court in Obtaining the Routing Information at Issue.

The exclusionary rule is a "judicially created remedy" that is "designed to deter police misconduct rather than to punish the errors of judges and magistrates." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984). "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." *Illinois v. Krull*, 480 U.S. 340, 347 (1987). The rule therefore does not apply "where [an] officer's conduct is objectively reasonable" because suppression "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." *Leon*, 468 U.S. at 919. For that reason, "evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Id.* (citation omitted).

This good-faith exception applies to "officer[s] acting in objectively reasonable reliance on a statute," later deemed unconstitutional, that authorizes warrantless administrative searches. *Krull*, 480 U.S. at 349. It follows *a fortiori* that officers act reasonably in relying on a statute that authorizes the acquisition of records only pursuant to an order issued by a neutral magistrate. The Supreme Court has explained:

> The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant. *Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law.* If the statute is subsequently declared unconstitutional, excluding evidence obtained pursuant to it prior to such a judicial declaration will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to enforce the statute as written. To paraphrase the Court's comment in *Leon*: *"Penalizing the officer for the [legislature's] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations."*

Krull, 480 U.S. at 349-50 (emphasis added).

Thus, even if the Court were to become the first to declare the Pen/Trap Act unconstitutional as applied to IP addresses, law enforcement was nonetheless entitled to rely on the strong presumption that statutes are constitutional. *See United States* v. *Watson*, 423 U.S. 411, 416 (1976) (applying a "strong presumption of constitutionality" when assessing challenges to a federal statute under the Fourth Amendment) (citation omitted). At the time the PRTT device was installed in this case, moreover, no binding appellate decision (or holding of any circuit) had suggested, much less held, that the Pen/Trap Act was unconstitutional as applied to internet routing information such as IP addresses. As discussed above, all federal authority was, and remains, to the contrary. Under such circumstances, "an officer cannot be expected to question the judgment of the legislature that passed the law" and therefore suppression "cannot logically contribute to the deterrence of Fourth Amendment violations." *Krull*, 480 U.S. at 349-50. *Cf. Davis v. United States*, 564 U.S. 229, 241 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule"). *See also, United States v. Russell Rose*, 914 F. Supp. 2d 15, 22-24 (D. Mass. 2012) (Gorton, J.) (applying *Davis* to deny motion to suppress warrantless GPS tracking evidence where officers

reasonably relied on non-binding precedent). Such reliance is all the more reasonable when law enforcement sought and obtained a court order from a neutral magistrate. Under such circumstances, suppression would serve no Constitutional interest.

E. The Government Complied With All Aspects of the Pen/Trap Act, the Stored Communications Act, and the Wiretap Act.

Gottesfeld claims that the installation of the PRTT in this case violated the Stored Communications Act ("SCA"), 18 U.S.C. § 2703. Dkt. #78 at 14. The SCA, however, is irrelevant to the installation and monitoring of the PRTT device. As described in Part II.A, *supra,* the Pen/Trap Act authorizes the installation of a PRTT device upon the government's certification that the information is "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122. No recitation of facts is required. Defendant simply conflates the two statutes, and the two separate standards they set forth for obtaining different types of information.

Because the defendant has not established a single instance in which "content" of his communications was obtained by the government, see Part II.C, *supra*, his claim that the PRTT violated the Wiretap Act must also fail.[5]

F. The Search Warrant Affidavit Established Probable Cause to Search Defendant's Residence Even Without the Pen Trap Data.

Even if the Court were, as Gottesfeld urges, to excise from the search warrant affidavit the results of the PRTT, the affidavit nonetheless established probable cause to search Gottesfeld's residence. In determining whether the excised affidavit established probable cause,

---

[5] The government notes further that defendant has not engaged the text of the Wiretap Act, nor the substantial body of case law devoted to interpreting the interception of electronic communications. "Few principles are more sacrosanct in this circuit than the principle that 'issues averted to in a perfunctory manner, unaccompanied by some effort at developed argumentation, are deemed waived.'" *Redondo-Borges v. U.S. Dep't of Hous. & Urban Dev.*, 421 F.3d 1, 6 (1st Cir. 2005) (quoting *United States v. Zannino*, 895 F.2d 1, 17 (1st Cir.1990)). This principal alone dooms his argument that the government's collection of IP addresses violated the Wiretap Act.

the question is whether a person of "reasonable caution" would believe that evidence of a crime would be found based on the affidavit included with the warrant. *United States v. Woodbury*, 511 F.3d 93, 98 (1st Cir. 2007).

Gottesfeld concedes that the affidavit established that he posted the YouTube video calling for action against Children's Hospital if it did not fire a particular doctor and discharge the teenage patient back to her family. Dkt. 78 at 16; Dkt. 78 Ex. 1, ¶¶ 16-18. More specifically, the affidavit establishes that, not only did Gottesfeld's YouTube account post the YouTube video, that video was posted from the IP address assigned to Gottesfeld's residence, meaning that someone at that residence "used a computer, tablet, smartphone, or other internet-enabled device" to post the video. *Id.* ¶¶ 16-18.

The affidavit also described that the video that Gottesfeld posted included a link to a posting, on the website pastebin.com, that listed detailed information about Children's Hospital's web server, including its IP address and server type. Dkt. 78 Ex. 1 ¶¶ 10-14. This is the server that was later attacked. When the hospital did not meet the demands set out in the video, the server identified in the pastebin.com posting was subjected to a distributed denial of service (DDOS) attack, which caused significant disruption to the hospital website and computer network. *Id.* ¶¶ 6-8.

The affidavit also described connections between Gottesfeld and other DDOS attacks against entities associated with what Gottesfeld called the "troubled teen industry." The affidavit described how Gottesfeld targeted a treatment center in Utah via social media accounts. *Id.*[6] ¶¶ 29-30. That treatment center then experienced a DDOS attack, as did the company that

[6] While they are included in the affidavit, which was filed under seal, the government has not publicly disclosed the names of these additional DDOS victims.

provided its records management. *Id.* ¶ 29. And the affidavit describes how Gottesfeld threatened to add a school-listing website to his campaign against the Utah treatment center if the website did not remove the center from its listings. *Id.* ¶ 31. That website, too, later suffered a DDOS attack. *Id.*

While these links to other DDOS attacks provide additional support for the probable cause finding, it is the direct connection between Gottesfeld's YouTube account and home IP address and the video threatening Children's Hospital (and the linked pastebin posting) that most directly establishes probable cause for the search. The threat and the linked pastebin posting, providing targeting information, are critical pieces of evidence of the crimes under investigation – not just the crime of damaging a computer (18 U.S.C. § 1030) but also the conspiracy among those responsible for threatening, organizing, and orchestrating this attack (18 U.S.C. § 371). *Id.* ¶ 2. By establishing that Gottesfeld's YouTube account posted the video from an internet-connected device at Gottesfeld's residence, the affidavit established probable cause to search that residence for that device and for other evidence and instrumentalities of these crimes.

G. <u>The Search Warrant Was Sufficiently Particular.</u>

In arguing that the search warrant was unconstitutionally overbroad, Gottesfeld misreads both the affidavit and the case law.

The Fourth Amendment requires that warrants particularly describe "the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The warrant in this case fulfilled this requirement. Attachment A to the warrant described in detail Gottesfeld's residence and included a photo. Dkt. 78 Attachment A. Attachment B to the warrant described in great detail the kinds of evidence to be seized. Dkt. 78 Attachment B. Specifically, section I of that attachment lists a series of people, entities, IP addresses, accounts, topics, location and identity information, and computer-specific evidence relevant to the crimes being investigated.

In support of his overbreadth claim, Gottesfeld focuses on the first sentence of section II of Attachment B, which authorizes the seizure of "[a]ll computer hardware (including smartphones and tablets), computer software, and storage media." Dkt. 78 at 17, Attachment B. But he neglects to mention the second sentence of that section, which states: "Off-site searching of these items shall be limited to searching for the items described in paragraph I." Nor does he mention that the affidavit describes in great detail, in paragraphs 34(a)-(b), why off-site searching of electronic devices is often necessary. Finally, while Gottesfeld criticizes the language in Affidavit paragraph 35 seeking permission to search and seize items "regardless of how their contents or ownership appear or are described by others at the scene of the search," he neglects to mention that the first three sentences of paragraph 35 explain why this is appropriate:

> The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant.

Dkt. 78 Exhibit 1 ¶ 35.

Gottesfeld bases his legal argument on the recent decision in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), but that case is distinguishable in many was from the situation presented here. In *Griffith*, police obtained a warrant to search the defendant's apartment in connection with their investigation of a homicide. *Id.* at 1268. The affidavit outlined evidence suggesting that Griffith was involved in the homicide and now lived in the apartment with his girlfriend. *Id.* at 1269. The affiant then relied on his training and experience and that of other officers to conclude that gang members maintain regular contact with each other and "often stay advised and share intelligence about their activities through cell phones and other electronic communication devices and the Internet, to include Facebook, Twitter and E-mail accounts." *Id.*

The affidavit then concluded: "Based upon the aforementioned facts and circumstances, and your affiant's experience and training, there is probable cause to believe that secreted inside of [the apartment] is evidence relating to the homicide discussed above." *Id.* In light of the paucity of the affidavit, the court, in *Griffith*, held:

> the affidavit supporting the warrant application provided virtually no reason to suspect that Griffith in fact owned a cell phone, let alone that any phone belonging to him and containing incriminating information would be found in the residence. At the same time, the warrant authorized the wholesale seizure of all electronic devices discovered in the apartment, including items owned by third parties. In those circumstances, we conclude that the warrant was unsupported by probable cause and unduly broad in its reach.

Id. at 1270-71.

The Gottesfeld affidavit could not have been more different from that in *Griffith*. It established that, not only did Gottesfeld's YouTube account post the YouTube video, that video was posted from the IP address assigned to Gottesfeld's residence, meaning that someone at that residence "used a computer, tablet, smartphone, or other internet-enabled device" to post the video. Dkt. 78 Ex. 1, ¶¶ 16-18. It also described how the PRTT records demonstrated that internet traffic from Gottesfeld's residence was using two anonymizing tools that were also being used by two Twitter accounts that were tweeting at or about the DDOS victims during and after the attacks. *Id.* ¶¶ 21-26. This affidavit, therefore, unlike that in *Griffith*, established probable cause that there were internet-capable devices in Gottesfeld's residence, that one or more of them would contain relevant evidence, and that it might not be possible to determine at the scene which device contained the relevant evidence. *Id.* ¶¶ 16-18, 21-26, 35.[7] The warrant in this case was, therefore, not unconstitutionally overbroad.

---

[7] *See United States v. McLellan*, 792 F.3d 200, 213 (1st Cir. 2015) (where there was one internet router for a residence, every internet connection established from any of the residence's computers would trace back to the same IP address).

H. Law Enforcement Relied in Good Faith on a Facially Valid Warrant.

Finally, even if this Court deemed the warrant deficient, "it could hardly be called so overbroad (or lacking in probable cause) 'as to render official belief in its [validity] entirely unreasonable.'" *United States v. Jenkins*, 680 F.3d 101, 107 (1st Cir. 2012) (quoting *Leon*, 468 U.S. at 923). This is a far cry from the rare case where a warrant is so clearly insufficient as to merit the "extreme sanction of exclusion[.]" *Leon*, 486 U.S. at 926. *Cf. United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993) (exclusion not proper where existence of probable cause was a "borderline call"); *United States v. Beckett*, 321 F.3d 26, 32-33 (1st Cir. 2003) (exclusion not proper even when evidence of nexus between criminal activity and residence was "less than overwhelming"). Because it cannot "be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment," *Leon,* 468 U.S. at 919, applying the exclusionary rule would not deter future Fourth Amendment violations and therefore is inappropriate in these circumstances, *Krull*, 480 U.S. at 347.

For all of these reasons, the Court should deny Gottesfeld's Motion to Suppress.

Respectfully submitted,

William D. Weinreb
Acting United States Attorney

By: */s/ Adam Bookbinder*
Adam J. Bookbinder
David J. D'Addio
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Adam Bookbinder

Dated: October 6, 2017

Exhibit Z

Monday, 09 October 2017

Exclusive: Court Documents Show Federal Wrongdoing, According to Wife of Suspected Hacker in Medical Kidnapping Case

Written by C. Mitchell Shaw

The federal case of an accused hacker illustrates the degree of malfeasance and underhanded tactics of the federal court system, according to the wife of that accused hacker.

Marty Gottesfeld is in prison awaiting trial on charges of hacking Boston Children's Hospital to save the life of a young girl. His wife, Dana Gottesfeld, has provided previously sealed court documents to *The New American*. She says those documents show that federal authorities "exceeded what they were legally allowed" to do in obtaining information about her husband's web traffic.

When Justina Pelletier's parents took the sick teenager to Boston Children's Hospital in February 2013, they had no idea the trip would result in a nightmare: the medical kidnapping of their daughter. They also had no idea that a man they had never met would later risk his own freedom to help Justina gain hers. That man — Marty Gottesfeld — believed he needed to act to save Justina's life. So as a senior systems engineer, he decided to apply his knowledge of computer systems to hit the hospital where it would hurt the most: On April 20, 2014, he knocked them off the Internet during a major fundraising drive.

When authorities — who had previously refused to investigate the claims of the Pelletiers and other families that the hospital had taken their children from them under false pretenses and that those children had been subjected to torture and other mistreatment — began to investigate the cyberattack, they looked at a YouTube video by someone claiming to be part of the hacktivist group Anonymous. That video, posted March 23, 2014, lays out the details of Justina's abuse at the hands of the state and the hospital. It

also lists links to information about the judge who issued the order terminating the parental rights of the Pelletiers, and to the doctor who ignored the diagnosis of the Pelletiers' family doctor that the teen suffers from Mitochondrial disease (claiming instead that she was suffering from a psychological disorder), the hospital, and the treatment center to which the hospital had transferred Justina (and where she continued to be denied medical treatment and the necessary pain medications for her disease and be subjected to what she and her family describe as torture).

Investigators were able to link the video to Gottesfeld since it was posted from an account he had signed up for and was posted from his IP address. Based on that, investigators obtained a "Tap and Trace" order to gather more information on Gottesfeld. In defiance of the fact that there is nothing in the video that would have satisfied the Fourth Amendment's requirement of "reasonable cause," investigators were able to convince a judge to sign off on the Tap and Trace order. So that order — made available here for the first time — was based on a video that should reasonably have been protected by the First Amendment.

The video provided contact information for people involved in Justina's medical incarceration and "implores" viewers to "use this information to your maximum potential in order to save Justina's life." The video specifically asks viewers to make phone calls and write letters. Despite the fact that later reports claim that the video called for viewers to hack the hospital, there is nothing in the video or the links that support those claims.

In fact, another recent case is worth a little comparison to this case. When a University of Wisconsin-Madison student posted a YouTube video showing black students beheading police officers wearing pig masks, there was no search warrant issued, no Tap and Trace, no arrest. Not even an investigation — though one state senator did call for one. While the UW-Madison student's video actually calls for violence, Marty's video calls for (gasp!) making phone calls and writing letters to ask the people responsible for torturing a sick child to stop that torture and let her go home to her loving family.

Even more importantly, though, Dana Gottsefeld told *The New American* in an exclusive interview that the search warrant based on the Tap and Trace order — and issued *after* that order was carried out — listed information about particular Internet traffic that was gathered by authorities "exceeding what the Tap and Trace allowed." She told us, "The search warrant affidavit [used to obtain the search warrant] mentions traffic obtained from the Tap and Trace. However the Tap and Trace, as ordered, shouldn't have given them those details."

So it appears that federal investigators — time after time, step after step — have trampled the Constitution to play a rousing game of persecution by prosecution of a man

who did what he did to defend a child's life. First, by honing in on Gottesfeld because of the video, then — if Dana Gottesfeld is correct (and it seems reasonable that she is) — by overstepping the boundaries of the Tap and Trace order obtained because of that video, leading to investigators obtaining a search warrant based on the information they gathered from that alleged overreach, and finally arresting Gottesfeld.

As to whether Gottesfeld did what he is accused of, the answer may be equally "yes" and "no." Gottesfeld issued a statement published by the Huffington Post nakedly titled "Why I Knocked Boston Children's Hospital Off the Internet." He lays out — in simple terms — both that he hacked the hospital's Internet server and — as the title implies — why he did it: "The defense of an innocent, learning disabled, 15-year-old girl."

As Dana explained to *The New American*, "We don't see the nexus of this case as 'Is the punishment too harsh for the crime?' — it's that it's not a crime in the first place." She went on to say, "When someone's life is at risk, the way Justina's was," Marty's actions — which would normally be criminal — are justifiable. "Let's say this wasn't a digital case; let's say this was in physical reality — in an alleyway or something. If you saw someone being hurt, you're allowed to take action to defend their life. It's called 'defense of others.' And when you do that — even if you use physical force, even if it's deadly force — it's not a crime." She added, "It's just because it's happening in cyber that it's more confusing."

After more than a year of Justina's parents fighting a losing legal battle to save their daughter as she grew increasingly sicker, and the hospital being able to weather the bad press, Marty hit them where they felt it. He took them offline in the midst of a fund drive.

Shortly after that, Justina was allowed to go home.

Marty wrote in the statement linked above:

> I also knew from my career experience as a biotech professional that no patients should be harmed if Boston Children's was knocked offline. There's no such thing as an outage-proof network, so hospitals have to be able to function without the Internet. It's required by federal law, and for accreditation. The only effects would be financial and on BCH's reputation.

As Dana explained to *The New American*:

> And that's really how we see this case — knocking a hospital off the Internet doesn't even hurt anybody. But it did apply the financial pressure that released her when her parents said her life was in danger and that they were afraid she was going to die.

As to whether there is a one-to-one, direct connection between Marty's hacking and Justina's release, Dana said:

> You can't isolate any one thing. There were a lot of people advocating for Justina. There were lawyers involved. But Boston Children's Hospital is largely untouchable. I mean, they can get bad press, but they're such a gigantic institution — just influentially — that bad press effects them a little, but hit them in their pocketbook and they're paying attention.

The prosecution — which, again, is building its case on the work of investigators who appear to have trampled the law underfoot to pursue this case — seems to have also drawn a connection between Marty's actions and Justina's release: They don't even want her mentioned in the case. As Dana told us, "The prosecution is motioning to exclude Justina from being mentioned at trial," adding, "They're trying to narrow the scope and exclude Justina from testifying — from really getting into her story."

And the impropriety and malfeasance doesn't stop there. The Tap and Trace order was not issued by a full judge, but by a federal magistrate. And it was not even the magistrate assigned to Gottesfeld's case. As constitutional lawyer and regular contributor to this magazine, Joe Wolverton, explains, "It's increasingly normal" for magistrates to issue these orders, though "it's not supposed to be that way." He points to the FISA court as an example of this "new normal" where "they do it completely secretly." Wolverton added that having federal magistrates issue these types of orders "is one of those things that have gone on for so long that you can't even get conservatives who want to rein that in."

As for prosecutors having the Tap and Trace signed by a magistrate who is not even assigned to the case — in a move that appears to indicate "judge shopping" (or in this case, magistrate shopping) — Wolverton said, "Now see, that's a different thing," adding, "That's not normal at all." He went on to tell *The New American* that "federal procedure says that if prosecutors have to go to another judge, you have to transfer the case." But in Gottesfeld's case, prosecutors shopped for another magistrate to sign off on the Tap and Trace and then continued to have the original magistrate work the case. Wolverton said these steps by the prosecution are "actionable" but "not likely to go anywhere" because "they'll look at you and say, 'Yeah, great, you're right. But so what?' and nothing will happen."

Dana Gottesfeld agrees. She told *The New American*, "That's federal court in a nutshell. In 2012, the federal courts had a 93 percent conviction rate — which is insane — because most people take plea deals" while prosecutors break rule after rule to secure those astronomically high conviction rates.

So while the prosecution seeks to control both the narrative and what the jury will be allowed to know and also continues to bend the procedures of federal prosecution to near the breaking point, Dana is working to raise awareness of her husband's plight,

because no one should face the prospect of a 15-year prison term for trying to save the life of a child. As part of Dana's efforts to raise awareness, she has much more information available at www.FreeMartyG.com and has coordinated with *The New American* to publish these newly released documents which are linked here as PDFs and on the FreeMartyG Instagram account.

Please review our Comment Policy before posting a comment

This is a complicated case I've written about before and it reeks of cronyism and corruption. The power structure in Boston is determined to prosecute Gottesfeld for orchestrating a direct denial of service attack on the hospital's online donation portal but has shown no interest in investigating or prosecuting anyone for the violation of Justina Pelletier's human rights or the rights of her parents.

Here is the audio recording the FBI is objecting to.

FBI admitting no investigation into Boston Children's Hospital or ...

Dana has email evidence as well as an invoice proving that she obtained the recordings legally through official channels, all of which leads her to believe the FBI is attempting to intimidate her. Her husband released a statement via Facebook accompanied by the recording.

> "If the people of America trust you with a badge and you hear of a child being tortured, then you are supposed to use that badge to protect that child. It's called the duty to act. Fidelity, Bravery, and Integrity. Three words lost on these Boston FBI agents who are protecting the people who abducted and tortured young Justina instead of Justina and her family."
> –Martin "MartyG" Gottesfeld

As I wrote once before, the issue for me here isn't whether or not Marty Gottesfeld broke the law. The issue is the selective prosecution of a man who was acting in response to a gross violation of human rights that hasn't even been investigated because the powerful are protecting each other while doing nothing for the real victim, Justina Pelletier.

TAGS: BOSTON CHILDREN'S HOSPITAL CORRUPTION CRONYISM DANA GOTTESFELD HARVARD MEDICAL SCHOOL JUSTINA PELTIER MARTY GOTTESFELD MEDICAL KIDNAPPING SELECTIVE PROSECUTION

Don't Let Iran Become the Next North Korea

Dan Spencer

FCC Commissioner to Trump: First Amendment, Baby! Learn to Love it!

Susan Wright

Trump's Cheap "Merry Christmas" Christianity Continues to Sway Evangelicals

Kimberly Ross